Universidad
Carlos III de Madrid

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería de Sistemas de Comunicaciones

TRABAJO FIN DE GRADO

DISEÑO DE UN IP BACKBONE MPLS

Autor: Ignacio Sánchez Cerro
Tutor: Víctor Pedro Gil Jiménez
Año: 2015

RESUMEN

A día de hoy, un *smarthphone* es miles de veces más potente que la tecnología de la NASA en 1969 cuando el Apollo 11 conquistó por primera vez la luna. Esto es un claro ejemplo de cómo la tecnología ha crecido en cuestión de unas pocas décadas lo que no ha hecho en millones de años. Aunque haya un pequeño número de personas que siga dudando de este hecho, lo que resulta innegable es el impacto que está teniendo en esta generación el uso de la tecnología y es aquí donde las telecomunicaciones juegan un papel crucial.

Este constante crecimiento provoca que la tecnología esté en continuo avance dejando rápidamente atrás tecnologías obsoletas incapaces de soportar lo que dicho crecimiento supone. Esto se refleja en el mundo de las telecomunicaciones lo que implica la expansión de infraestructura para cubrir dichas necesidades. En ocasiones, basta con adaptar las nuevas mejoras a la estructura existente pero, en otros casos, es necesario un cambio de topología.

Este proyecto trata del último aspecto, en el que se pretende renovar desde cero una arquitectura nueva capaz de integrar en una sola topología servicios de voz y datos móviles y fijos, e incluso TV.

Para ello, este documento plantea el diseño de una red *IP Backbone MPLS*, en el que se reflejan las diferentes alternativas a nivel de hardware, el diseño de la solución aportada y las ventajas de la tecnología MPLS aplicables al diseño elegido.

ABSTRACT

Nowadays, a *Smartphone* is infinitely more powerful that the technology of NASA in 1969 when the Apollo 11 reached the moon for the first time. This is a clear example of how technology has grown just in a few decades, what it hadn't grown in millions of years. However, even though a small group of people still doubt about this fact, the impact that the use of technology is having in this generation is undeniable and it is here where telecommunications play a crucial role.

This constant growth implies that technology is in continuous development quickly leaving behind older technologies making them obsolete. These technologies are not able to support the growth that this constant change implies, thus this is reflected in the telecommunications world, it clearly needing an improvement and expansion of infrastructure to be able to cover this necessities. In some cases, for this change to take place it is enough to adapt the existing structures to the improvements, yet for other a complete change in topology is required.

This project deals with the later. In it, it is intended to create a completely new architecture that will be able to integrate in an only topology voice and data, mobile and fix and even TV services.

In order to do so, this document sets out the design of an IP Backbone MPLS network, where the different alternatives in terms of hardware are presented as well as the design of the chosen solution and the advantages that the MPLS technology offers them applied to the design in question.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INDICE DE COMANDOS

1. INTRODUCTION

1.1 Motivation

This project describes part of an extensive project at Vodafone S.A.U. Spain, in which I am currently working. The purpose of it is to provide a detailed low-level description of the architecture and logical design of an IP Backbone based in MPLS.

The constant evolution of technology and the exponential growth of it in recent years, not only has an enormous impact on the people's behaviour, but it also affects directly to the telecommunications world, which nowadays represents an essential part of our lives.

In fact, this change is such, that some of the current communication systems are becoming obsolete and therefore need to be replaced with more innovative technological items. This is one of the factors that push telecommunications to the necessity of dealing with this issue and being at the forefront in this field. In some cases, just a small part of the technology needs to be adapted with the newest improvements, but unfortunately this is not the case of this project, that implies a complete *face washing* in terms of technology.

1.2 Objectives

Once we have taken into account the conditions mentioned above, we need to know where we come from. The background of this project is a network, in which the services delivered in the end to customers are in separate networks. This is why the aim and purpose of this project is to create from scratch a complete network in which these services, such as Internet, fixed and mobile voice and data and even TV, are merged into a single topology, optimizing the network with the newest technology and minimizing the costs of the previous one.

Therefore, we aim to achieve a unique globally aligned architecture for the transport of the previous services between the Core and rest of the network, enabling both the distribution and aggregation layer. This architecture will count with several sites spread all over Spain and Portugal them being interconnected.

Since this project means a complete restoration, it involves the continuous and coordinated work of a variety of partners and departments. These, come from the project management, the feasibility of it in terms of financial funds, an analytic perspective, the design and implementation, and the duty of the sales team, among others.

This document, it will only consider the design and the implementation of the architecture, from the engineering point of view, analysing the alternatives of the hardware equipment, the low-level design based on the MPLS advantages and the final architecture topology, leaving apart the security that implies.

1.3 Regulatory framework

One of the most important aspects that sometimes might go unnoticed is the necessity of a regulatory framework in order to deal with the issues that the telecommunication world has to undertake.

Thus, to solve these existing problems, Europe is regulated by the *Telecoms Package*, approved by the European Parliament, so that all members of the European Union should operate under its mandatory compliance.

Spain, however, is regulated by the *Ley General de Telecomunicaciones (LGTEL),* created in May 2014. This law represents the highest standards in order to the sector of the network and electronic communication services as a whole. Audio-visual communication services as well as the Information Society are however not regulated under this law but by different entities. *{7} {9}*

One of the objectives of the Government is to enhance the legal security, because it lumps together the current standards in terms of national and international fields.

The organism in charge of the management of the changes in the existing law is the Industry, Energy and Tourism Ministry, and with the support of the *Comision Nacional de los Mercados y la Competencia (CNMC)* will establish a law reform. *{8}*

The most important features of this law are the following:

- A more effective use of the radio spectrum in order to facilitate the deployment of the wireless broadband.
- Promote an open Internet to everybody thanks to *network neutrality.*
- The defence of the consumers interests in terms of election, price and quality.
- Decrease and simplify the existing regulations about operators and telecommunication companies.

Last but not least, a key point to be considered in the *Telecoms Package*, is the progressive elimination of *roaming*, an aspect that is not reflected in the LGTEL. In Spain, the enormous benefits coming from this part, due to the amount of tourism all over the country, lead to a non-regulation unless it is imposed by the European Parliament.

1.4 Socioeconomic environment

As we have stated, it is clear that technology is in continuous development and is precisely here where telecommunications play a crucial role. It is important to mention as well the increase, not only nationally but internationally; that this field is facing what should be called the technological age. This is why enterprises should take into consideration some factors that they should be more than aware of.

Among these tendencies, it is possible to highlight the following:

- Mobile
    - By mid-2014, the number of people with Internet access from mobile devices exceeded the number of fixed users.
    - An average of 50% of users utilizes one or more Internet access devices, such as tablets, watches, GPS, etc.
    - The improvement in comfort and speed leads to the fact that the majority of information is made by such devices.
    - The *Smartphone sales* was four times the previous year's.

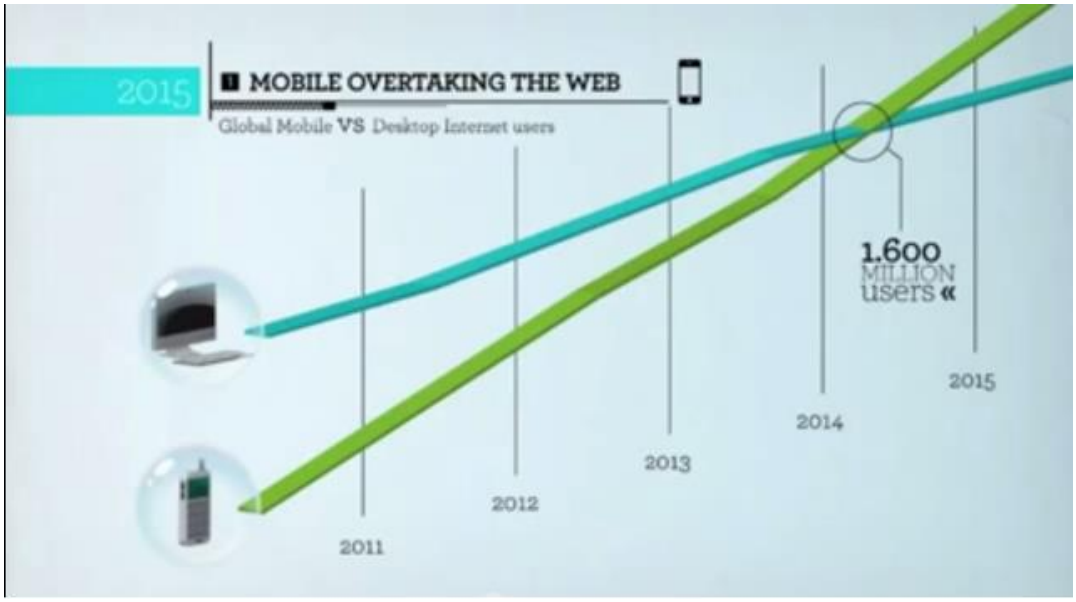


Figura1: Internet móvil vs fijo

- Social Networks
    - 100 hours of video are uploaded every minute to Youtube.
    - 93% of companies use social networks to promote themselves.
    - An average of 2 users join Facebook every second.

- Cloud-computing
    - It is estimated that cloud-computing is the third factor that better helps boost economic growth in Spain.
    - Represents an environment to optimize the harnessing of the IT Services in terms of business management.

Besides, it is expected that the evolution of these tendencies will lead to a new generation, commonly known as *Internet of things,* based on the capacity and interconnection of anything with Internet access.

These aspects have one thing in common: the massive usage of information. This concept is known as *Big Data*, which should be regulated by the State and it is here where telephone operators and the *OTT (Over the top)* suffer the most. *{16}*

From the point of view of the Information Society in Spain, it is important to highlight several points that lead to the need of this project.

First of all, a decrease in incomes due to the economic crisis that Spain is facing impacts consumers directly and consequently their savings. Besides, it contributes to the appearance of the *Mobile Virtual Network Operators (MVNO)*, these having better offers than the big operators.

Secondly, the constant growth in the mobile broadband network forces the requirement of an increase in terms of infrastructure, apart from competitiveness in speed. In addition, the fixed telephony has been diminished by the abovementioned MVNO.

These factors lead to the aim of this project, which is the integration of all services, converging in a single network. The advantages from the customer's point of view are the following:

- Multiple accesses across the network no matter the location, either by optical fiber, FTTH (*Fiber to the Home), ADSL/VDSL,* and mobile.
- Leading-edge technology and high performances for the transmission of data at a great speed and a guaranteed quality of the services delivered.
- High flexibility, which enables the possibility to accommodate the requirements of every site and adapt to the connectivity necessities.
- Secure and protected access to your private network from any place in the world.
- Prioritisation of the traffic depending on the critical applications.

1.5 Structure of the paper

This document is structured as follows:

- Chapter 2, "*ESTADO DEL ARTE*", analyses the evolution of technology in the telecommunications field and briefly explains MPLS, the technology in which this project is based.

- Chapter 3, "*HERRAMIENTAS*", explains the tools used in the implementation of the project.

- Chapter 4, "*ARQUITECTURA PROPUESTA*", consists on the Hardware Overview. It also contemplates the different alternatives, proposes a possible architecture and shows the protocols that should be used in the network.

- Chapter 5, "ARQUITECTURA DEFINITIVA" is the most important and thus the largest chapter in the whole paper. It includes the following content:

    - First of all, once the architecture requirements have been analysed, the final decided architecture is carried out as well as the physical deployment of it. This part includes the different equipment for each service containing the information of transmission too.

    - Secondly, the location of the different sites spread all over the topology is shown.

    - The third part details the transmission infrastructure.

    - The fourth part contains the addressing and naming of the network.

    - The fifth part of this chapter represents the *Control Plane,* in which it is provided a low-level technical design of the MPLS technology applied to the network implementation.

    - The sixth part includes the *Quality of Service* that the network will apply depending on the different services offered. It contains a detailed explanation on how the traffic is treated.

    - To sum up, the last part "*Gestión y mantenimiento de la Red*" encompasses the tolls required for the management of the whole network, including data bases.

It is important to mention, that despite the fact that both the fifth and the sixth parts could have been included in the second chapter, *"Estado del arte"*, they belong to this chapter because they are not only explained but at the same time they are related to the architecture design.

In addition, this chapter includes command configuration of the final architecture design.

- Chapter 6, "*Conclusiones*" shows the conclusions of the project implementation and the scalability in the future.

- Chapter 7, "*Presupuesto*", includes the economic part where the budget of the project is presented.

- Chapter 8, "Summary", contains a summary of the whole project.

- Chapter 9, "*Referencias Bibliográficas*", the bibliographical references used in the realization of this project are highlighted.

- Chapter 10, *"Glosario"* is referred to the glossary of the project, which contains and defines the most frequent terms of the whole paper.

2. ESTADO DEL ARTE

La tecnología sobre la cual se basa la red es MPLS (*Multiprocol Label Switching*) por lo que, a pesar de que en apartados posteriores la explicaremos más detalladamente, es importante tener una visión general acerca de sus principales características y su funcionamiento. Para ello, nos remontaremos a los antecedentes de esta tecnología y analizaremos el porqué de la aparición de la misma.

El continuo crecimiento de Internet desde sus inicios, además de la demanda de nuevos servicios, tales como aplicaciones multimedia con necesidades de ancho de banda y una consecuente calidad de servicio, supuso la creación de tecnologías que lidiaran con este problema, surgiendo así la introducción de IP desarrollada a mediados de los años 90.

En ella, IP (*Internet Protocol)* fue conquistando terreno como protocolo de red frente a tecnologías anteriores como SNA (*Systems Network Architecture*), IPX (*Internetwork Packet Exchamge)*, AppleTalk y OSI (*Open System Interconnection)*, entre otras. A diferencia de las anteriores, IP, permitía mediante protocolos de enrutamiento, funciones de direccionamiento, creando tablas de enrutamiento basándose en las direcciones IP para direccionar el tráfico. Gracias al uso de protocolos, como RIP (*Routing Information Protocol)*, IGRP (*Interior Gateway Routing Protocol)* y OSPF (*Open Shortest Path First)*, todos ellos de nivel 3, los routers eran capaces de establecer comunicación entre sí con el fin de actualizar y mantener sus tablas. Pero era tal el auge de Internet, que dicho protocolo rápidamente generó una saturación de los proveedores de servicios debido a la necesidad de ancho de banda.

Es por ello, por lo que surgió la aparición de la tecnología IP/ATM (*Asynchronous Transfer Mode)*, la cual se basó en la combinación de ambas tecnologías siendo una eficiente alternativa durante los primeros años, incluso facilitando la entrada de los operadores telefónicos. Dicha tecnología, permitió los beneficios de superponer ambas, aprovechando la infraestructura ATM existente, cubriendo la falta de ancho de banda a precios competitivos y obteniendo a la vez, la rapidez en el transporte de datos gracias a los conmutadores ATM. Ésta, se basaba en el envío de celdas a través de la conmutación de etiquetas mediante los propios conmutadores. Permitía además, la separación en distintos niveles, del *routing* IP y la conmutación, en los niveles 3 (control y envío de paquetes) y 2 (control, señalización y envío de celdas) respectivamente. No obstante, la tecnología IP sobre ATM contaba también con ciertas limitaciones, puesto que la expansión sobre una topología virtual superpuesta, así como la complejidad de la gestión de dos redes separadas y tecnológicamente distintas, supuso un coste excesivo para los proveedores de servicio.

La continua convergencia hacia IP de las aplicaciones del momento, sumada a las dificultades de rendimiento de la tecnología IP/ATM, propició durante 1997 y 1998, que una serie de fabricantes lidiaran con el problema anterior, desarrollando técnicas para la integración de los niveles 2 y 3. Dichas técnicas, denominadas *IP Switching y Multilayer Switching,* conmutación IP y conmutación multinivel respectivamente, fueron adoptadas por empresas privadas, en las que cabe destacar IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba. La combinación de todas ellas, condujeron a la creación en 1998 por parte de la IETF de un único estándar, apareciendo por tanto, la tecnología MPLS definida en la RFC 3031.

MPLS es un mecanismo de transporte de datos que opera entre la capa de enlace de datos y la capa de red del modelo OSI y a diferencia de sus predecesores, permite aprovechar lo mejor de ambas capas. Por tanto, MPLS se basa en dos componentes fundamentales, la separación entre las funciones de *routing* (control) y *forwarding* (reenvío) y, al igual que ATM, MPLS hace uso del intercambio de etiquetas para el envío de datos.

La parte de control se encarga de las decisiones de encaminamiento, mediante los protocolos OSPF, IS-IS (*Intermediate system to intermediate system)* y BGP (*Border Gateway Protocol)*, para el intercambio de información con los otros routers, pero no construye una tabla en la que consultar la dirección IP de los paquetes que llegan, sino que informa a la parte de reenvío que construye una tabla de etiquetas. El único router que tiene que hacer las funciones de enrutamiento es el primero que debe decidir qué etiqueta colocar para cada paquete.

En cuanto a la etiqueta, es un campo de 32 bits, que se añade a la cabecera del paquete y que identifica una *FEC (Forwarding Equivalent Class)*, un conjunto de paquetes que se envían sobre el mismo camino a través de una red. La FEC es el nombre que recibe el tráfico que se encamina bajo una etiqueta. En la siguiente figura, se puede apreciar una etiqueta MPLS, con cada uno de sus campos.

Figura 2: Campos de la etiqueta MPLS

- Etiqueta: campo que identifica una FEC formado por 20 bits.
- Exp: 3 bits experimentales destinados a la calidad de servicio.
- S: bit indicador de final de pila en cuyo caso tendrá un valor de 1. En el resto de los casos será 0.

- TTL: tiempo de vida de la etiqueta. Representa el máximo número de saltos que puede dar el paquete antes de que sea descartado. Está compuesto por 8 bits.

Una de las características más importantes de MPLS, es la capacidad de añadir una cabecera a cada paquete, pero ésta puede contener una o más etiquetas siguiendo un mecanismo *LIFO (Last in First Out)*, de ahí que se conozca con el nombre de *label stacking* o pila de etiquetas, expuestas como ejemplo, en la figura que viene a continuación.

Figura 3: Pila de etiquetas

Sobre dichas etiquetas se pueden realizar una serie de operaciones, entre las que se distinguen las siguientes:

- *PUSH*: se encarga de añadir una nueva etiqueta a la pila.
- *SWAP*: reemplaza la etiqueta en la cima de la pila de etiquetas, con una nueva etiqueta específica.
- *POP*: extrae una etiqueta de la pila.

Normalmente, las operaciones de *SWAP* y *PUSH* se realizan conjuntamente.

Otra de las mejoras de MPLS frente a las tecnologías de las cuales procede, es la posibilidad de transmisión de datos basados en cualquier tecnología de transporte, ya sea ATM, *Frame Relay*, PPP (*Point-to-Point Protocol)* o Ethernet entre otras. Si el protocolo de transporte de datos contiene un campo para las etiquetas, como es el caso de los dos primeros, se utilizaban dichos campos para las etiquetas. Pero para las tecnologías que carecían de esta ventaja, MPLS emplea una cabecera genérica de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

Estas etiquetas se encapsulan en las cabeceras de los paquetes que son enviados entre los distintos routers, conocidos en MPLS como *LSR (Label Switch Router)* y dependiendo de su funcionalidad, distinguimos tres tipos:

- *Ingress* LSR: también conocido como *LER (Label Edge Router),* es el router a la entrada encargado de la asignación de la primera etiqueta.
- *Intermediate* LSR: son todos los routers entre medias cuya función reside en recibir las etiquetas de los LSR anteriores y añadir una nueva para pasar el paquete al siguiente LSR.
- *Egress* LSR: último router, responsable de quitar la etiqueta. Al estar en el otro extremo, este tipo de routers también son considerados como LER.

El conjunto de LSRs por los que pasan los paquetes desde su origen a su destino, forman un camino que en MPLS se denomina con el nombre de *LSP (Label Switch Path)*. El primer router del LSP, será por tanto el *Ingress* LSR, el último el *Egress* LSR y el resto que intervienen en dicho camino serán los LSRs intermedios. Es importante mencionar que los LSPs son unidireccionales, a no ser que el tráfico sea dúplex, en cuyo caso se empleará un LSP para cada sentido. *{2}*

Dentro de un LSP, se reenvían los paquetes etiquetados a través de la red MPLS, en el que a diferencia de una red IP, en la cual se analiza exclusivamente la dirección IP, las etiquetas se consultan en la *LFIB (Label Forwarding Information Base)*, y comprobando la etiqueta externa el LSR sabrá como reenviar el paquete y hará uso de las operaciones comentadas anteriormente. El LSR es capaz de distinguir si el paquete recibido está etiquetado o si carece de ella, es decir, si se trata solamente de un paquete IP. En el caso de que un LSR reciba un paquete IP (*Ingress* LSR) lo reenvía etiquetado, método que se conoce como *IP-to-label*. Si un paquete ya etiquetado es recibido por un LSR, dependiendo de si se trata de un *Egress* LSR o uno intermedio, podrá o bien quitar las etiquetas y reenviarlo como un paquete IP o reenviarlo como un paquete etiquetado. El primer caso se conoce como label-to-IP mientras que el segundo de ellos, *label-to-label*. Cada paquete, por tanto, se envía de un LSR a otro creando saltos o *hops,* dentro del LSP.

Una característica común en las redes MPLS, es lo que se conoce como *penultimate-hop-popping (PHP).* Esto es, que el LSR anterior al *Egress* LSR, debe enviar los paquetes sin etiqueta con el fin de que el *Egress*, solamente reciba un paquete IP y no sea necesario realizar dos búsquedas, una en la LFIB para averiguar que la etiqueta debe ser eliminada, y otra por IP para reenviar dicho paquete. Por tanto, si la etiqueta es eliminada el penúltimo nodo, solo se deberá llevar a cabo la segunda de ellas. *{2}*

El funcionamiento de MPLS se basa en dos protocolos de distribución de etiquetas, *RSVP (Resource Reservation Protocol) y LDP (Label Distribution Protocol)*.

El primero de ellos se fundamenta mediante una reserva de recursos para ejecutar la distribución de las etiquetas sobre MPLS. No obstante, RSVP por sí solo carece de mucha función por lo que hace uso de una de las principales ventajas de MPLS, la ingeniería de tráfico o RSVP-TE *(Traffic Engineering)*, detallado en IETF RFC 3209. Una de sus características más importantes es que permite el re-enrutamiento de los túneles LSP, con el propósito de dar una solución ante caídas, congestión y cuellos de botella. RSVP-TE soporta además la creación de rutas explícitas con o sin reserva de recursos teniendo en cuenta parámetros tales como el ancho de banda disponible, con el fin de optimizar los recursos. RSVP no solo se usa para hacer ingeniería de tráfico puesto que otro de sus prestaciones es *Multiprotocol BGP (MP-BGP)* cuya función es la distribución de etiquetas solo para las rutas de BGP. *{2} {3} {5}*

En cambio, LDP, a diferencia de RSVP, se encarga de distribuir las etiquetas para las rutas interiores. Por ello, todos los LSRs deben establecer sesiones LDP entre ellos. Entre sus funciones cabe destacar:

Descubrimiento de los LSRs que operen según dicho protocolo.

- Establecimiento y mantenimiento de las sesiones.
- El anuncio de etiquetas.

Para la primera de sus funciones, aquellos LSRs que ejecuten el protocolo LDP, se encargan de enviar unos mensajes conocidos con el nombre de *hello*, a todos los enlaces que tengan este protocolo activado. Si el primer nodo recibe un mensaje hello de vuelta se establece una sesión LDP entre ellos. En caso contrario, no se establecerá ninguna. No obstante, es importante mencionar, que este tipo de mensajes cuentan con un tiempo de vida determinado y hay que fijar con cautela dicho intervalo para evitar que sea demasiado bajo y demasiado alto.

Una vez establecida la sesión LDP entre ambos LSRs, mediante una conexión TCP (*Transmission Control Protocol*), se fijan una serie de parámetros, que explicaremos con más detalle más adelante.

Tras el cumplimiento de las dos primeras funciones, entra en juego el anuncio de asociación de etiquetas, que corresponde a la tarea principal de LDP. Dentro de este apartado, se pueden distinguir varios modos de distribución de etiquetas.

Modo de distribución

- *Downstream-on-demand*: cada LSR solicita a su siguiente salto, sobre un LSP, una etiqueta de asociación local para esa FEC.
- *Unsolicited Downstream*: un LSR puede distribuir asociaciones de etiquetas a LSRs adyacentes aunque no lo hayan solicitado.

LSP Control

- Ordenado: el nodo solo realiza una asociación local de etiquetas para una FEC concreta si es el *Egress* LSR para el FEC o si el LSR ha recibido una asociación desde su *next-hop* para este FEC.
- Independiente: cada LSR toma su decisión de asignación FEC de manera independiente, pero esto hace que permita una convergencia más rápida al hacerlo con el *routing* IP. Lo malo es que puede provocar inconsistencias de etiquetado.

Modo de retención

- Liberal: cada LSR mantiene las asociaciones entre una etiqueta y su FEC de todos los LSRs por los que la ha recibido, aunque no corresponda con la de su siguiente salto.
- Conservativo: Solo mantiene la entrada correspondiente a su siguiente LSR o *next-hop.* El resto se descartan enviando un mensaje conocido como *Label Release*.

Otra de las mejoras que brinda MPLS es la calidad de Servicio o *QoS (Quality of service)*, en el que las etiquetas permiten gestionar prioridades entre los paquetes de la red, garantizando una serie de niveles de calidad determinados.

Por último y no por ello menos importante, sino todo lo contrario, MPLS cuenta con una prestación que la hace lo más característico frente a sus antepasados y son las VPN (*Virtual Private Networks)* MPLS o redes privadas MPLS. Una VPN es una red que emula redes privadas virtuales sobre una infraestructura compartida, con funcionalidades de red y de seguridad, equivalentes a las que se obtienen con una red privada, pero pudiendo tener el tráfico totalmente separado. Una de las ventajas que presenta frente a las redes IP tradicionales es que desvincula el plano de control del plano de tráfico gracias a que dispone de una red MPLS por debajo. Su objetivo es el soporte de aplicaciones intranet y extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables.

En la siguiente imagen, podemos observar el esquema de una VPN MPLS en el que los clientes sin estar conectados directamente gozan de las ventajas, como si de una red local se tratara. Los PE son los routers conocidos en MPLS como los *Provider Edge y los* router de los clientes son denominados CE (*Customer Edge).*

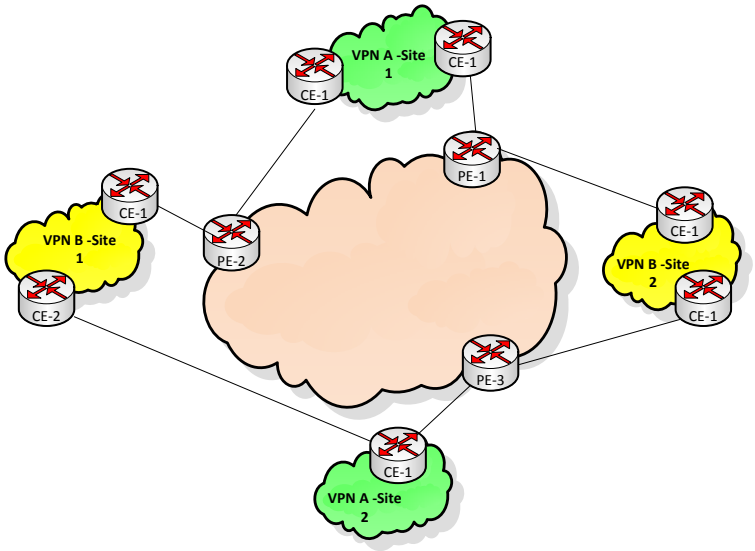


Figura 4: Ejemplo VPN MPLS

3. HERRAMIENTAS

Las herramientas necesarias para la realización de este proyecto son las siguientes:

3.1 Secure CRT 7.0

Esta herramienta es un emulador de terminal, capaz de soportar *Secure Shell* (SSH) y posee además todas las funciones de Telnet, incluyendo *logins* automáticos, nombrado de sesiones para diferentes hosts, etc. Esta aplicación se encarga de la gestión y la configuración de los equipos de la red, además de sus nodos e interfaces. Toda la configuración de comandos a lo largo de la este documento ha sido realizada desde esta herramienta.

3.2 Microsoft Visio 2010

Las figuras de los esquemas de red han sido generadas a partir de esta herramienta, ofreciendo una visión bastante detallada del escenario de red.

4. ARQUITECTURA PROPUESTA

La necesidad de la integración de los servicios en las redes convergentes da lugar a la demanda de un nuevo tipo de router, conocido como router de servicio o *service router.* Este tipo de router es un router orientado a Internet que ofrece servicios de *best-effort* y permite la migración de los servicios tradicionales de voz y datos en una misma topología. Su función no solo engloba la parte anterior, pues además debe tener la capacidad de satisfacer el tema de la privacidad de datos, voz y video en una única red e infraestructura optimizada, Maximizando la sencillez pero minimizando costes al mismo tiempo.

Este tipo de servicios, tales como redes punto a punto, *VPLS* (*Virtual Private LAN Service)* multipunto y *VPN*s permiten a la red, tener un amplio elenco de proveedores de *Hardware* a un precio mínimo ofreciendo a la vez flexibilidad y calidad a nivel de usuario.

Debido a la alta competitividad entre los distintos proveedores que nos ofrecen sus productos para llevar a cabo la implementación y el despliegue físico de nuestra red, siendo mínimas las diferencias tanto a nivel técnico como económico, y teniendo en cuenta todas las especificaciones e información necesarias, se ha decidido a través de una *RFQ,* como proveedor de *Hardware* a Alcatel-Lucent. *{6}*

4.1 *Overview del Hardware*

Una vez elegido a Alcatel-Lucent como proveedor de Hardware y antes de decidir la arquitectura definitiva, examinaremos los distintos routers junto con sus prestaciones y especificaciones técnicas para cada tipo de servicio.

Se ha decidido no contar con los equipos más novedosos puesto que están en una fase experimental de prueba y no están totalmente comercializados. No obstante, los equipos vigentes a día de hoy satisfacen perfectamente las necesidades propuestas y será cuestión de tiempo estos equipos sean sustituidos por los aquellos más novedosos.

4.1.1 Router 7750 SR Tecnología Fast Path

Los equipos 7750SR tienen la capacidad de dar un soporte de rendimiento desde los 10 Gbps a los 1000Gbps. Esto se basa en la tecnología conocida como *Flexible Fast Path* (FP), la cual se caracteriza por un *NPA* (*Network Processor Array*), es decir, un tipo de procesador totalmente programable.

Este tipo de equipos cuentan con dos tipos de *Fast Path*:

- FP I: Habilitado con tarjetas de tipo IOM2, que incorpora puertos de 10 Gb cada uno. El total de los módulos de I/O (entrada/salida) tendrán 20 Gbps, por lo que en su totalidad, es decir, con el límite de tarjetas de tipo IOM2, el equipo albergaría un máximo de 200 Gbps.
- FP II: Dentro de este tipo de modalidad, hay que distinguir dos subcategorías de tarjetas.
    - Habilitado con tarjetas de tipo IOM3-XP, engloba solo un tipo de puertos con un *throughput* o rendimiento de 50 Gbps. En el caso de su máxima ocupación, el *throughput* total sería de unos 500Gbps.
    - Habilitado con tarjetas de tipo IMM, que al igual que las anteriores, tienen un *throughput* de 50 Gbps cada una. La diferencia con respecto a las del tipo IOM3, es la mejora de tener 20 Gbps, por lo que el equipo ascendería a un límite de 1000Gbps.

Este tipo de diseño de tarjetas, representa una considerable mejora frente a otras como *Asics*, cuya falta de programabilidad hace de esta tecnología, inferior con respecto a la FP y un tipo de procesadores normales, siendo notable la diferencia en cuanto a rendimiento se refiere.

Con una arquitectura óptima para el tratamiento de paquetes, este tipo de tecnología alcanza satisfacer un rendimiento más que adecuado, en el que los equipos 7750 SR son capaces de combinar tanto la velocidad como la densidad de tráfico de una manera altamente eficaz tanto a nivel tecnológico como económico.

4.1.2 Router 7750 SR-12

Dentro de los 7750 SR, están presentes más de una subcategoría de routers, siendo el 7750 SR-12 el primero de ellos.

Este tipo de router es el más grande de su familia y tiene un total de 12 ranuras de acceso de tarjetas, en el que dos de ellas están dedicadas a la redundancia del equipo en sí. Cada ranura o *slot*, cuenta con un *SF/CPM* (*Switch Fabric/Control Processor Module*), en el que solamente uno de ellos está destinado para el mantenimiento y las operaciones. Un segundo, proporciona la redundancia para el *SF/CPM*. Tres de ellas, permiten un rendimiento full dúplex de 200, 500 y 1000Gbsps. Cuando dos *SF/CPM* son instaladas, el tráfico se reparte entre ambas. Por ejemplo, dos *SF* de 200 y 500 Gbps pueden, o bien, proporcionar un rendimiento no redundante de 400 y 1000 Gbps respectivamente, o facilitar un rendimiento de 200 y 400 Gbps, en el que los 100 Gbps restantes pueden estar dedicados a la redundancia *full dúplex*. La utilidad de los otros 10 *slots* será para las tarjetas IOM.

El plano inferior, ofrece un rendimiento full dúplex de 40 Gbps para cada ranura IOM2, 50 Gbps para el caso de las IOM3-XP y 100Gbps para las de tipo de IMM.

Figura 5: 7750-SR 12

El SR-12 funciona con -48V DC o 220V AC. Las dimensiones físicas de dichos equipos, medidos en pulgadas, son de 24.5”H X 17.5”W X 25.25”D, donde H, W y D, son altura, anchura y profundidad, respectivamente. *{11}*

En la siguiente tabla, queda reflejada de manera más visual y concisa alguna de las características expuestas en el párrafo anterior.

Parámetros	Capacidad
Ancho de banda full duplex, no redundante	200G/500G/1000G Switch Fabric
	20G/50G/100G por ranura
	Redundancia en la *Switch Fabric*/CPU
I/O slots	10
Media Dependent Adapters (MDAs)	20
Redundancia	AC Power (1 + 1)
	DC Power (1 + 1)
	Switch Fabrics/Control Processor
	Módulos (*SF/CPM*)(1 + 1)

Tabla 1: Parámetros 7750-SR 12

4.1.3 Router 7750 SR-7

Este tipo de routers está compuesto por un sistema totalmente redundante, que cuenta con una capacidad de 7 slots. Dos de ellas están dedicadas a la redundancia del propio equipo, en el que cada una de ellas alberga un *SF/CPM*. Solo se necesita una *SF/CPM* para operaciones no bloqueantes a un rendimiento de 500 Gbps. Un segundo *SF/CPM* proporciona una completa redundancia. Cuando se instalan dos *SF/CPM*, el tráfico se reparte de manera balanceada entre ambos. El 7750 SR-7 puede ser inicialmente activado con un SW de 200 Gbps, el cual agrega el total de los Gbps anteriores cuando las tarjetas IOMs estén disponibles.

Figura 6: 7750-SR 7

En cuanto a la alimentación del 7750 SR-7, este equipo funciona con -48V DC o 120/240V AC. El tema de la conexión se lleva a cabo a través de la parte trasera mediante dos PEMs (*Power Entry Modules*). Sus dimensiones físicas son de 14”H x 17.5”W x 23.5”D.

Parámetros	Capacidad
Full-duplex, ancho de banda no redundante	200G/500G/1000G *Switch Fabric*
	20G/50G/100G por ranura
	Redundancia en la *Switch Fabric/CPU*
I/O slots	5
Media Dependent Adapters (MDAs)	10
Redundancia	AC Power (1 + 1)
	DC Power (1 + 1)
	Switch Fabrics/Control Processor
	Modules (SF/CPM)(1 + 1)

Tabla 2: Parámetros 7750-SR 7

4.1.4 Router 7710 SR

Este tipo de router es el primer de esta gama específicamente diseñado y optimizado para el transporte de datos, voz y video. El router 7710 ofrece un amplio conjunto de interfaces que otorgan un alto rendimiento a los servicios ofrecidos. Sus plataformas de software y su arquitectura hardware le permite ser uno de los mejores routers combinando alta capacidad y un servicio flexible y adaptable. Además, al igual que la gama de los 7750 SR, emplea la tecnología FP, en el que concentra tanto la velocidad como la densidad de los mejores switches, con la programabilidad y el procesamiento de paquetes necesarios para ofrecer servicios a una infraestructura basada en IP/MPLS.

La gama de 7710-SR dispone de una gran número de interfaces a través de las *CMAs* Compact Media Adapters y estándar *MDAs* (Media Dependent Adapaters) de la familia de los 7750 SR.

Dentro de este modelo, podemos distinguir a su vez, dos subcategorías, el 7710 SR-c12 y el 7710 SR-c4.

Entre las especificaciones del primero de ellos, cabe destacar su rendimiento, el cual asciende a 24 Gbps de capacidad. Se distinguen, además diferentes combinaciones en relación a sus CMAs/MDAs.

- Hasta 8 CMAs y 2 MDAs.
- Hasta 6 CMAs y 3 MDAs.
- Hasta 4 CMAs y 4 MDAs.
- Hasta 2 CMAs y 5 MDAs.
- Hasta un máximo de 6 MDAs.

El equipo funciona con un sistema de alimentación de -40V a -75V en DC o entre 85 y 265 V en AC. Sus dimensiones físicas alcanzan 8.7”H, 17.5”W y 23.6”D.

Figura 7: 7710-SR c-12

En cuanto al segundo, cuenta con una capacidad de *throughput* de 18 Gbps half-duplex. Su relación CMAs/MDAs se distribuye de la siguiente forma:

- Hasta 4 CMAs.
- 1 MDA y hasta 2 CMAs.
- Hasta 2 MDAs.

Los sistemas de alimentación del equipo son idénticos a los del modelo anterior. Sus dimensiones físicas, en cambio, son inferiores, 5.3”H, 17.5”W y 22”D. *{12}*

Figura 8: 7710-SR c-4

4.1.5 Router 7950 XRS-20

Este tipo de routers revoluciona la parte de Internet, ofreciendo hasta 5 veces más de la capacidad del resto de routers alternativos, consumiendo al mismo tiempo solo una tercera parte de la electricidad.

Cuenta con un total de 80X100GE puertos y tiene la oportunidad de doblar dicha capacidad, ya que dispone de la posibilidad de interconectarlo con otro 7950 XRS. Está diseñado además, para alcanzar 40 Tbps individualmente con una futura expansión de 240 Tbps para el caso de una configuración múltiple.

Estos tipos de routers están creados para dar servicios de video, aplicaciones en la nube, y una cantidad masiva de datos multimedia. Al mismo tiempo, el coste se ve reducido con respecto a sus competidores.

La distribución de las CMAs y SFMs es la siguiente:

- 6 C-XMAs de 2x100GB.
- 9 C-XMAs de 20x10 GB.
- 2 CPMs y 8 SFMs.

Con respecto a su arquitectura, en la siguiente imagen podemos ver la parte delantera y trasera del equipo junto con cada parte descrita. Sus dimensiones físicas alcanzan las 19”H, 5”W y 5”D. *{13}*

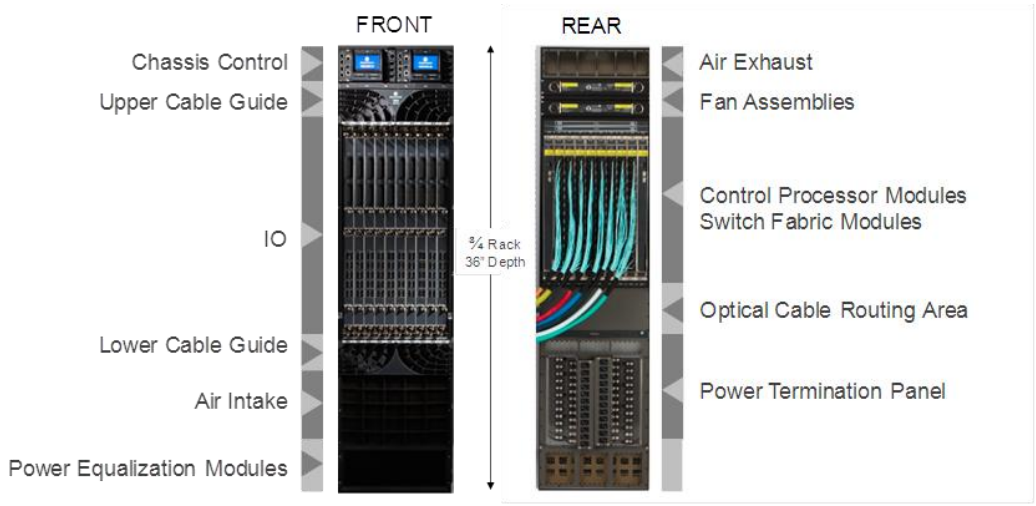


Figura 9: 7950 XRS-20

4.1.6 Alcatel-Lucent 1675 LambdaUnite MultiService *Switch*

En cuanto a la parte del transporte para la sección de transmisión de datos, contaremos con el modelo de Alcatel-Lucent 1675 LambdaUnite MSS. Éste, supone la siguiente generación de enlaces de conmutación ópticos de 10GB y 40 GB que proporcionan una amplia amalgama de aplicaciones en una topología en forma de anillo y malla, manteniendo a la vez una red flexible, eficiente en coste y sencilla de maniobrar. Además, facilita la integración de servicios Ethernet en redes backbone aplicables a la tecnología SONET/SDH.

Figura 10: 1675 LambdaUnite MSS

Sus niveles de potencia oscilan entre -40V y -72 V en DC y 60/48 V en AC. Sus dimensiones físicas son de 37.5”H, 19.7”W y 21.5”D. *{14}*

4.1.7 Equipo 1830 Photonic Service Switch

En cuanto a la parte la capa de transporte para la sección de transmisión de datos, los equipos 1830 PSS representan la siguiente generación de WDM, ofreciendo multiservicio de transporte desde el Core al resto de la red. El 1830 PSS transforma el tradicional WDM en una flexible capa de transporte ágil a nivel de fotónica, conmutación multicapa y ofrece servicios como si de una red inteligente se tratara. La plataforma T/ROADM provee un elenco de aplicaciones y servicios, tales como Carrier Ethernet, *backhaul* móvil y vídeo *multicast*.

Estos equipos brindan la posibilidad de evolucionar del acceso compacto a conmutación Terabit OTN, además de alcanzar una mejora en las capacidades fotónicas. El PSE (*Photonic Service Engine*), habilita enlaces de 100 GB y un camino de 400 GB a nivel de transporte. Aprovechando un plano de control inteligente y haciendo uso de datos integrados, el 1830 PSS simplifica el mantenimiento de la red optimizando la eficiencia y el rendimiento multicapa. La capacidad por cada *slot* es de 60GB.

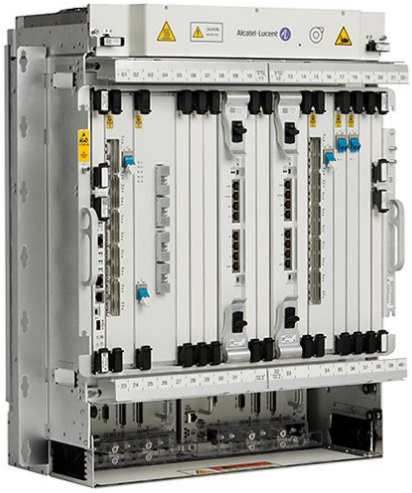


Figura 11: 1830 PSS

Estos equipos funcionan con un sistema de alimentación de -48 V en DC o 115/240 V en AC y sus dimensiones físicas alcanzan las 24.5”H, 19”W y 12”D. *{15}*

4.2 Capa de Core

La capa del núcleo de la red o *Core*, se encarga de proporcionar conectividad entre las capas de distribución y agregación, además de suministrar una alta velocidad y redundancia a la hora de mover paquetes entre los equipos de la capa de distribución de las diferentes zonas de nuestra red. Los routers y switches de la capa de Core son

los más potentes puesto que deben ser los que soporten la mayor cantidad de tráfico y por tanto un número elevado de conexiones, pero asegurando a la vez seguridad y redundancia.

Los routers Core de nuestra red, es decir los *Provider routers*, que llamaremos P routers a partir de ahora para abreviar, están distribuidos de manera simétrica para asegurar resistencia y redundancia desde capas de distribución y agregación remotas.

Los enlaces entre los distintos routers P, o PP (*Provider P*) son de Nx10Gb/s y la mayoría de los enlaces de acceso al Core, *PE (Provider Edge)* con PP, son de Nx10Gb/s salvo algunas excepciones de centros pequeños, en los que no serán necesarios tanta capacidad y estarán limitados. No obstante, debido a una funcionalidad de limitación de velocidad del modelo 7750-SR, la capa de transmisión se verá afectada reduciendo la velocidad de dichos enlaces.

Una vez analizadas las especificaciones y características de los equipos en los apartados anteriores, se propone llevar a cabo la implementación de los 7750 SR-12 para el Core de nuestra red. En consecuencia, dichos equipos deben ser capaces de soportar una serie de protocolos que explicaremos más en detalle en apartados posteriores.

- IS-IS
- LDP
- RSVP-TE

Para la parte del acceso a Internet, se plantea la utilización de los 7950 XRS-20 puesto que al ser los de mayor capacidad estarán perfectamente preparados para soportar el tráfico proveniente de Internet. Contaremos con dos grandes centros que serán los que sirvan de Gateway o interconexión entre los PEs y la red exterior.

Además, se hará uso de tres *Route Reflectors (RR)* o reflectores de rutas, cuya función es precisamente reflejar las rutas y contiene Internet *full-routing*. Entre sus otras funciones, cabe destacar la de distribuir rutas BGP VPN-IPv4 y VPN-IPv6 a los PE-As, PE-Cs y a los PE-Es formando así la capa de distribución y agregación en cada centro. Por tanto, a diferencia de los PEs, nunca descartan rutas VPN-IPv4. Dos de los tres RR estarán conectados a los 7950 XRS-20 mencionados en el apartado anterior, mientras que el tercero de ellos estará destinado para la parte del Core.

Es importante que se tenga constancia de que este tipo de routers no se encargan de enrutar ningún tráfico de cliente y estarán colocalizados a los routers P, mediante uno o más enlaces Gigabit Ethernet. Para la implementación de los *Route Reflectors*, se sugiere la gama del modelo 7710-SR, sobre los cuales deberán configurarse los siguientes protocolos:

- IS-IS
- BGP (*Multi Protocol* iBPG) a los PE-A y a los PE-C.

De dichos protocolos, es significativo mencionar que las sesiones de BGP solo serán de tipo IP.

4.3 Capa de distribución y agregación

Esta capa de red se encarga del *routing*, el filtraje y de la aplicación de las políticas de calidad de servicio. Entre sus funciones de agregación destacan las de minimizar el coste por puerto y la de conexión con sus clientes.

4.3.1 Arquitectura entre PEs

Esta capa está formada por PE-Cs en cada centro, conectados de manera simétrica a dos PPs, ya sean mediante Nx1 GE o Nx10 GE. Con el fin de reducir costes, se ha decidido integrar, para algunos centros, las funciones de los PE-Cs y los PE-As en un mismo equipo 7750-SR. En cambio, habrá centros en los que los PE-A estén presentes de manera independiente. Un ejemplo individual de la arquitectura entre los PPs y los PEs se puede observar en la siguiente figura.

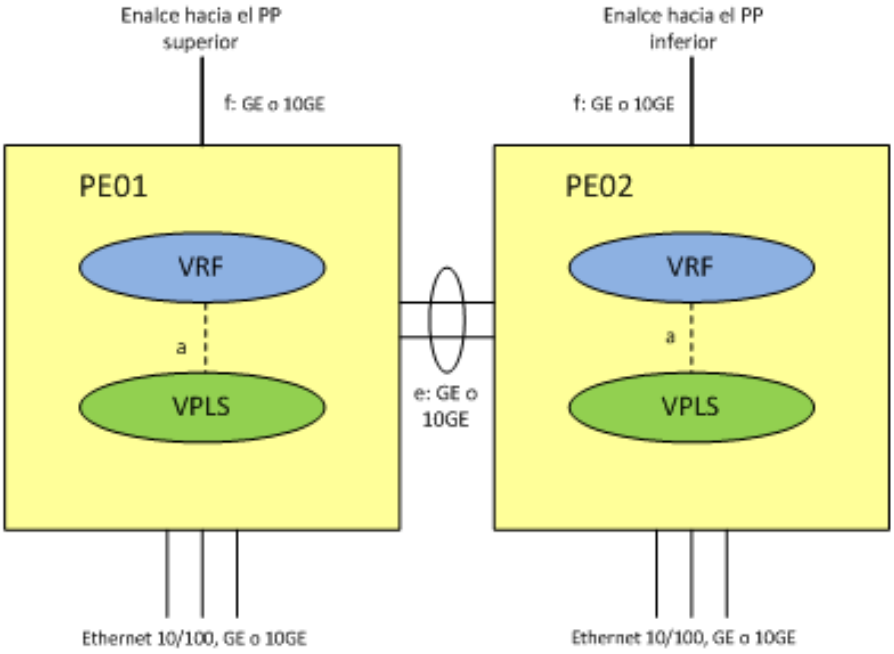


Figura 12: Arquitectura PP-PE

En la figura anterior se distinguen las siguientes interfaces:

- *Interfaz a:* sirve de interconexión entre, o bien, una VPLS con una VPRN o entre dos VPLS a través de un enlace físico.
- *Interfaz e*: implementado a través de enlaces de Nx1GE o Nx10GE basados en el sistema 802.3ad. Dichos enlaces lógicos interconectan las VPLS de cada PE provisionando un puente entre las VPRNs. En caso de fallo, el enlace lógico será enrutado directamente al router P para asegurar la conectividad.
- *Interfaz f*: enlace que interconecta los PEs con los PPs, es decir, con el Core de la red. Estos enlaces pueden ser de tipo Nx1GE o Nx10GE, dependiendo del tamaño y el tráfico cursado de cada centro.

Se han de establecer una serie de protocolos, sobre los cuales los routers deben ser capaces de soportar:

- ISIS
- LDP en todas las interfaces
- RSVP-TE en todas las interfaces
- *Multi-Protocol* BGP a los *Route Reflectors*

4.4 Servicios de red

La arquitectura expuesta en el apartado anterior debe ser capaz no solo de transportar todo tipo de servicios sino de asegurar una calidad de servicio óptima para ellos. Por tanto, se han de cumplir una serie de requisitos:

- Asegurar fiabilidad de *SIGTRAN* y servicios de voz.
- Mejorar los mecanismos de retardo del tráfico.
- Optimizar tanto las operaciones en la red, como el coste de transmisión entre nodos, manteniendo un balanceo de tráfico para evitar saturación.

Según este tipo de servicios, debemos diferenciar dos tipos de servicios dependiendo de su importancia frente a fallos:

- Servicios de tipo 1: aquellos más sensibles en cuanto al *jitter* o pérdida de paquetes.
- Servicios de tipo 2: aquellos más sensibles en latencia.

4.5 Protocolos

Tal y como hemos visto en los apartados anteriores, la red albergará cinco tipos de routers, los PCs, los PEs (PEs, Internet PEs, y PE-E) y los RR. Para cada uno de ellos, y sus consecuentes utilidades, deberán estar preparados para soportar una serie de configuraciones y operar conforme a unos protocolos, que previamente hemos comentado. En la siguiente tabla quedan reflejados para cada tipo de router, dichos protocolos necesarios que tendrán que utilizar.

	7950XRS PE-C	7750SR PE-C	PE-A	PE-E	PP	RR
LAG	S	S	S	S	S	N
ISIS	S	S	S	S	S	S
BGP	S	S	S	S	N	S
MPLS	S	S	S	S	S	N
LDP	S	S	N	S	S	N
RSVP_TE	S	S	S	S	S	N
QoS	S	S	S	S	S	S
Servicios L2VPN	S	S	S	S	N	N
Servicios L3VPN	S	S	S	S	N	N
Security-filters	S	S	S	S	S	S

Tabla 3: Protocolos por cada tipo de router

5. ARQUITECTURA DEFINITIVA

Tras haber analizado en el apartado anterior los distintos tipos de equipos con los que se puede contar y después de haber comentado brevemente el diseño de la arquitectura, en esta sección se decide finalmente tanto la arquitectura definitiva como los equipos a utilizar.

5.1 Configuración de elementos de red

En este apartado se pretende detallar la configuración física de la red, analizando por separada cada uno de los elementos que la componen, además de las interfaces de interconexión entre cada uno de los anteriores y los protocolos que deben operar.

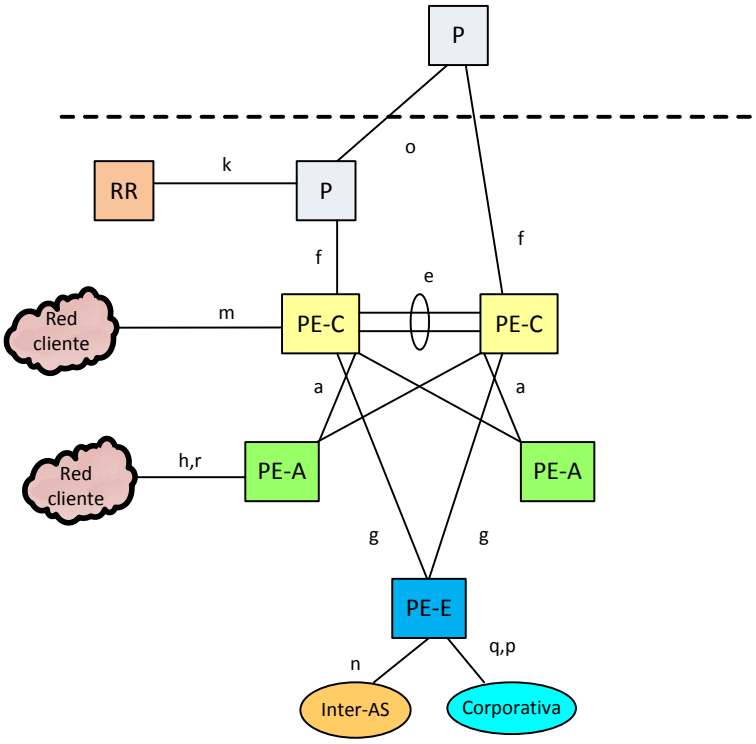


Figura 13: Configuración física de la red

A partir de ahora, la estructura de la red, sin contar con la parte de Internet, la denominaremos con el nombre de **ISNET**.

5.1.1 Router P

Para la parte del Core, tal y como se ha mencionado en el apartado 2.2, se emplearán los routers de la gama 7750 SR-12, cuya interconexión entre ellos estará basada en enlaces de 1X10 GE, con la posibilidad de aumentarlos a Nx10GE en caso de saturación por incremento de tráfico.

En la siguiente tabla se refleja de forma más concisa y clara las prestaciones de cada interfaz.

Interfaz	Destino	Número	Capa física	Óptica	Enlace de datos	Encapsulado	Protocolos
o	P	3	N x 10GE	LW/LR	Ethernet	MPLS	ISIS, LDP, RSVP-TE
f	PE-C	Número de centros en cada zona	N x 1GE o N x 10GE	LW/LR o LX	Ethernet	MPLS	ISIS, LDP, RSVP-TE
k (3 x P)	RR	1	1GE	LX	Ethernet	MPLS	ISIS

Tabla 4: Configuración física de los routers PP

5.1.2 Routers PE-C

5.1.2.1 Router PE-C Core

Los routers que se conectan directamente al Core, al igual que éste, serán del modelo 7750 SR-12.

Interfaz	Destino	Número	Capa física	Óptica	Enlace de datos	Encapsulado	Protocolos
f	P	≥1	n x 1GE o n x 10GE	LX o LW/LR	Ethernet 802.3ad	MPLS	ISIS, LDP, RSVP-TE
a	PE-C (VPRN a VPLS)	≥1	n x 1GE o n x 10GE	LX o LW/LR	Ethernet 802.3ad	-	VRRP
a	PE-A (VPLS a VPLS)	≥2	n x 10GE	LW/LR	Ethernet	MPLS	ISIS, RSVP-TE , MP-IBGP, LACP
e	PE-C	≥2	n x 1GE o n x 10GE	LX o LW/LR	Ethernet 802.3ad	MPLS	ISIS, RSVP-TE, LDP, MP-IBGP, LACP
m	Cliente	≥2	Fast/GigE/ 10GigE	TX, LX o LW/LR	Ethernet	-	OSPF, BGP, VRRP

Tabla 5: Configuración física de los routers PE-C

5.1.2.2 Router PE-C Internet

Para los routers PE-C destinados para la parte de Internet, a diferencia de los convencionales, se utilizarán el modelo 7950-XRS.

Interfaz	Destino	Número	Capa física	Óptica	Enlace de datos	Encapsulado	Protocolos
f	P o PE-C	≥1	N x 10GE	LX o LW/LR	Ethernet 802.3ad	MPLS	ISIS, LDP, RSVP-TE
e	7950XRS PE-C	≥2	N x 10GE	LX o LW/LR	Ethernet 802.3ad	MPLS	ISIS, RSVP-TE, LDP, MP-IBGP, LACP
m	Cliente	N	10GigE	TX, LX o LW/LR	Ethernet	-	OSPF, BGP, VRRP

Tabla 6: Configuración física de los routers 7950-XRS

5.1.3 Routers PE-A

Los routers de tipo PE-A pertenecerán, al igual que los PE-Cs convencionales y los del Core, al modelo 7750-SR 12.

Interfaz	Destino	Número	Capa física	Óptica	Enlace de datos	Encapsulado	Protocolos
a	PE-C (VPLS a VPLS)	≥2	N x 10GE	LW/LR	Ethernet	MPLS	ISIS, RSVP-TE , MP-IBGP, LACP
h, r	Cliente	N	GigE	TX	Ethernet	-	LACP

Tabla 7: Configuración física routers PE-A

5.1.4 Routers externos PE-E

Los routers externos están destinados para dar cobertura a los servicios corporativos de la red. Para ello, se contarán con los routers de tipo 7750 SR-12 con capacidad de enlaces de Gigabit Ethernet, puertos STM-1 E1 o E3.

Los clientes que requieran encriptación de tráfico, se les será otorgado mediante MDA *IPSec.*

Interfaz	Destino	Número	Capa física	Óptica	Enlace de datos	Encapsulado	Protocolos
g	PE-C	≥1	n x 1GE	LX	Ethernet 802.3ad	MPLS	ISIS, RSVP-TE, LDP, MP-IBGP, LACP
q	Cliente	-	-	-	-	-	IPSec, BGP
p	Cliente	-	STM-1	TX	SDH	-	OSPF, BGP
n	Inter-AS (*Autonomous System*)	≥1	n x 1GE	LX	Ethernet 802.3ad	MPLS	MP-EBGP, LACP

Tabla 8: Configuración física routers externos

5.1.5 *Route Reflectors*

Tal y como se ha comentado en el apartado 2.2, se contará con 6 RRs, la mitad de ellos para la parte de Internet y los tres restantes para la parte del Core. Sus funciones, entre otras, son la propagación de rutas VPN-IPv4 y VPN-IPv6 entre los PEs a través del multiprotocolo iBGP (*internal* BGP). Puesto que el uso de estos RRs, elimina la necesidad de un mallado completo de iBGP entre los PEs, como contraposición introduce ciertos puntos de fallo. Es por ello por lo que se van a desplegar estos 3 últimos usando el modelo 7710-SRc12, mientras que para la parte de Internet se llevarán a cabo routers 7750SR.

Interfaz	Destino	Número	Capa física	Óptica	Enlace de datos	Encapsulado	Protocolos
k	P	1 o 2	GigE	LX	Ethernet	MPLS	ISIS, MP-iBGP

Tabla 9: Configuración física Route Reflectors

Para aclarar ciertos conceptos de las tablas anteriores, se definen los siguientes:

- *LX*: un tipo de multiplexación por división de longitud de onda para distancias entre 240 m y 300 m sobre fibra óptica multi-modo. También admite hasta 10 km sobre fibra mono-modo. Usa longitudes de onda alrededor de los 1310 nm.
- *LR*: estándar que permite distancias de hasta 40 km sobre fibra mono-modo, usando de 1310 a 1550nm. Recientemente, varios fabricantes han introducido interfaces de hasta 80 km.
- *LW*: variedad de multiplexación que usa *WAN PHY* (capa física), se basa en una trama ligera *SDH/SONET.* Se corresponden en el nivel físico con LR.

5.2 Centros

Una vez visto la topología general de cada tipo de router, la siguiente tabla muestra el nombre de los centros según el tipo al que pertenezcan.

Centro	Core	RR	7950XRS PE-C	7750SR PE-C	PE-A	PE-E	Z1	Z2	Z3	Z4	Z5	Z6
Móstoles	✠	✠	✠	✠		✠	✠					
Moncloa				✠	✠		✠					
San Sebastián de los Reyes	✠	✠	✠	✠			✠					
Plaza Castilla				✠			✠					
Barcelona				✠				✠				
Pamplona				✠	✠			✠				
Vitoria	✠	✠		✠				✠				
Zaragoza				✠		✠		✠				
Castellón				✠	✠				✠			

Valencia	✠	✠		✠					✠			
Murcia				✠					✠			
Alicante				✠					✠			
Sevilla				✠	✠					✠		
Málaga				✠		✠				✠		
Granada	✠	✠		✠						✠		
Córdoba				✠		✠				✠		
Lisboa	✠	✠		✠							✠	
Oporto				✠	✠						✠	
Coimbra				✠		✠					✠	
Braga				✠							✠	
Vigo				✠								✠
Oviedo				✠		✠						✠
Pontevedra				✠	✠							✠
Salamanca				✠								✠

Tabla 10: Centros de ISNET

Una vez decididos los equipos definitivos para cada tipo de router y su función, se deberá decidir la arquitectura de la red. Teniendo en cuanto la necesidad de redundancia y simetría de la misma, se ha optado por aplicar una topología en forma de prisma triangular para la parte del CORE, tal y como se muestra en la siguiente figura.

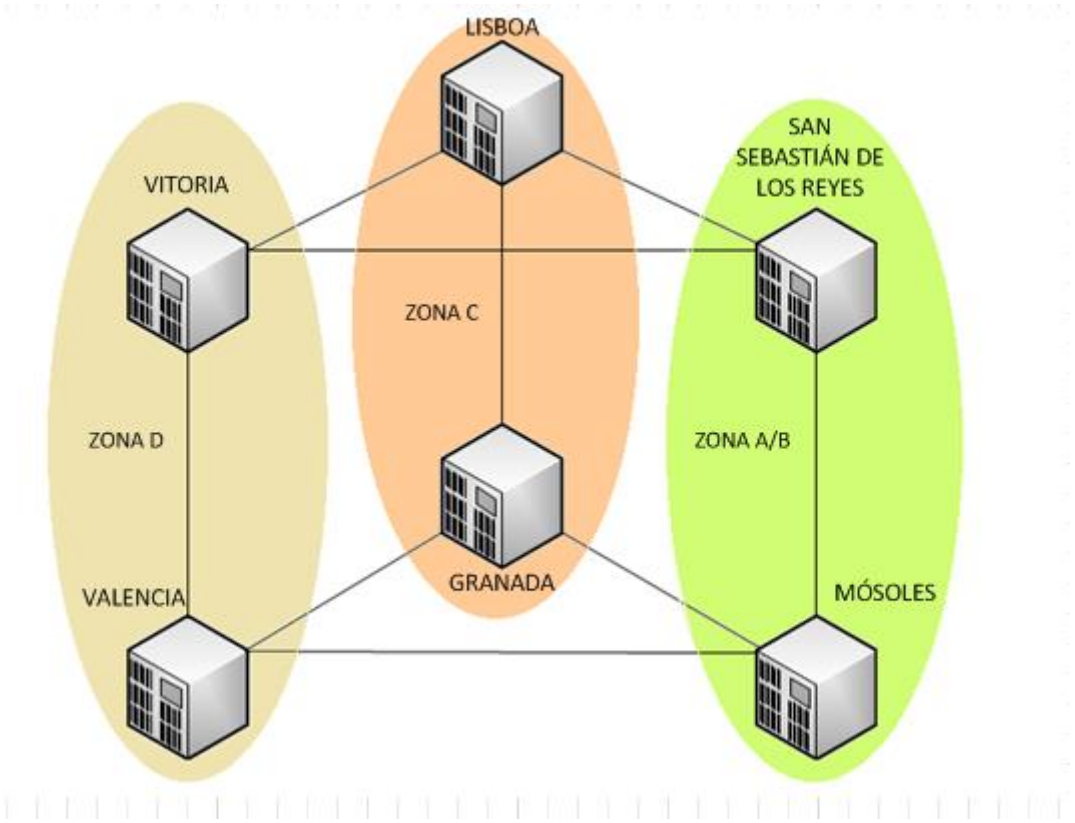


Figura 14: Esquema del Core

La conexión de los PE-C con los PP del Core se establece según las zonas determinadas, siguiente la tabla anterior.

- Los centros de la zona 1 y 2 se conectarán con la zona A/B.
- Los centros de la zona 3 y 5 se conectarán con la zona C.
- Los centros de la zona 4 y 6 se conectarán con la zona D.

Para la parte de Internet, la mitad de los 24 centros tendrán acceso a Internet (ver tabla 19), por lo que estarán conectados a los PE-Cs 7950-XRS, que serán los que lleven toda la parte de Internet, tanto fijo como móvil. Tal y como se puede ver en la figura 15, por cada centro, se conectarán dos PE a cada PP dependiendo de la zona a la pertenezcan estos últimos, ya sea A/B, C o D. Para la parte de Internet ocurre de igual manera, es decir, de los 12 centros con conexión a los 2 routers 7950 XRS, un PE se conectará a uno de los 7950, mientras que el otro se conectará con el 7950 restante.

Esto arquitectura queda reflejada en la siguiente figura:

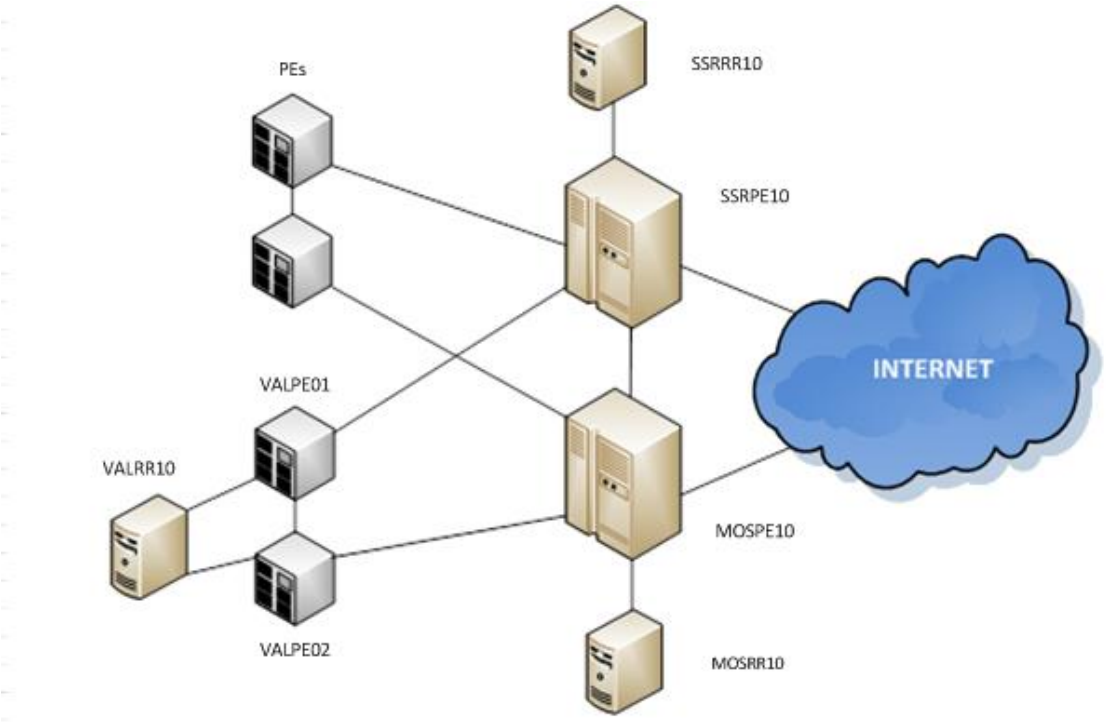


Figura 15: Esquema Parte Internet

Como resumen, se contará con el siguiente número de equipos:

- 6 Route Reflectors, tres de ellos para la parte de Internet (7750 SR) y otros tres para conectados al Core (7710 SR), ver tabla 10.
- 6 PPs, que formarán la parte del Core, usando el modelo 7750 SR.
- 48 PE-Cs conectados a los PPs, es decir, dos PE-Cs por cada centro (ver figura 15), sumando los 24 centros de la figura 10.

- 6 PE-A, uno por cada zona, también de la gama 7750 SR.
- 6 PE-E, formados por routers 7750 SR.
- 2 PE-C de la parte de Internet (ver figura 18), implementados por routers de la gama 7950 XRS.

5.3 Infraestructura de transporte

En esta sección se pretende analizar la parte del transporte de datos a través de la red, examinando y detallando los elementos necesarios para ello.

5.3.1 Transmisión

La infraestructura en cuanto a la transmisión se refiere, está basada en Alcatel-Lucent 1675 Lambda Unite MSS (SDH), WaveStar OLS 1.6 T/Alcatel-Lucent DWDM y equipamiento 1830 PSS.

Todas las interfaces entre los routers de la Red y la topología de transporte estarán implementados basándose en enlaces o bien Gigabit Ethernet, 10 Gigabit Ethernet o 100 Gigabit Ethernet, que serán entregados sobre SDH/DWDM, directamente conectando los equipos 7750-SR/7950-XRS a Alcatel-Lucent 1675 Lambda Unite MSS o a los equipos 1830 PSS, expuestos en los apartados 2.1.6 y 2.1.7 respectivamente.

Según la topología en la figura 12 y las tablas del apartado anterior, podemos resumir los siguientes enlaces:

- ***P - P:*** Nx10GE
- ***PE-C - P****:* Nx1GE o Nx10GE
- ***PE-C – PE-C***: Nx1GE o Nx10GE basados en IEEE 802.3ad LE (hasta un máximo de 32xGE)
- ***7950-XRS PE-C - 7950-XRS PE-C***: Nx1GE o Nx10GE basados en IEEE 802.3ad LE (hasta un máximo de 32xGE)

En cuanto a la interconexión de los PPs con los PEs, para aquellos centros más pequeños en los que el tráfico cursado sea bajo, es decir, que el ancho de banda requerido de sus enlaces sea inferior al del puerto físico, la transmisión se entregará siguiendo un número determinado de VC4s.

Para determinar el número de VC4s a otorgar, se deberá contar con un modelo y una estimación del tráfico que se cursará por dicho enlace, manteniendo un margen del 20% de seguridad en caso de un crecimiento inesperado, pero a la vez evitando malgastar recursos innecesarios. Puesto que el uso de estos VC4s, desde el punto de vista de los routers, supone una limitación de los enlaces con respecto al enlace físico real, en este caso de los 1x10GE, el modelo 7750-SR dispone de una restricción frente

al equipo de transmisión, configurando dicha limitación por debajo de la velocidad física del enlace.

Para llevar a cabo el transporte de datos, se deben cumplir unas determinadas especificaciones ópticas en cuanto a la transmisión se refiere, tal y como aparecen en la siguiente tabla.

Especificaciones	1000Base	1000Base	1000Base	1000Base	10GBASE	10GBASE	10GBASE
Nombre	SX	LX	EX	ZX	SR	LR	ER
Longitud de onda	850nm	1310nm	1310nm	1550nm	850nm	1310nm	1550nm
Distancia	500m	10km	40km	70km	200m	10km	40km
Potencia de arranque (Máx) en dBm	-3.0	-3.0	+3.0	+5.0	-1.2	+0.5	+4.0
Potencia de arranque (min) en dBm	-11.5	-11.5	-1.0	0	-7.3	-8.2	-4.7
Potencia recibida(máx) en dBm	0	-3.0	+1.0	-3.0	-1.0	+0.5	-1.0
Potencia recibida (min) en dBm	-17.0	-19.0	-21.0	-23.0	-9.9	-14.4	-15.8

Tabla 11: Especificaciones ópticas Ethernet

5.3.2 Protección SDH

La infraestructura de la parte de transmisión está fusionada con ISNET, por lo que están presentes varios Shared Risk Link Groups (SRLGs) o grupo de enlaces de riesgo compartido. Esto supone que un fallo dentro de la red de transmisión puede no solo afectar a un enlace entre routers P, sino a enlaces entre PE-C y P.

La red de transmisión no satisfará una total protección a todos los caminos SDH que transporten enlaces de ISNET.

En la siguiente tabla se muestra el esquema de protección que se seguirá entre la parte de transmisión e ISNET.

Enlace	Plano	Zona	Protección	Modo
Core	-	-	ISNET	802.3ah
Acceso	Superior	Z1	SDH	1+1
Acceso	Inferior	Z1	ISNET	802.3ah
Acceso	Superior	Z2	SDH	1+1
Acceso	Inferior	Z2	ISNET	802.3ah
Acceso	Superior	Z3	ISNET	802.3ah
Acceso	Inferior	Z3	SDH	1+1
Acceso	Superior	Z4	SDH	1+1
Acceso	Inferior	Z4	ISNET	802.3ah

Acceso	Superior	Z5	ISNET	802.3ah
Acceso	Inferior	Z5	SDH	1+1
Acceso	Superior	Z6	SDH	1+1
Acceso	Inferior	Z6	ISNET	802.3ah

Tabla 12: ISNET-SDH esquema de protección

5.3.3 Detección de fallo

Al haber SRLGs, será más que probable la aparición de fallos, por lo que ante la posibilidad de que eso suceda, dicho fallo dependerá del tipo de enlace, según sea:

- *SDH:* A través del propio enlace o *LPT (Link Pass Through)*
- *DWDM:* Fallo de propagación como si de una fibra respaldada se tratase.

En el caso de DWDM, esto ocurre como si fuera una fibra directa, pero tests realizados sobre SDH han observado que los tiempos de LPT son tolerables para los servicios críticos.

EFM OAM o 802.3ah será el protocolo para detectar los fallos SDH y recuperarse mediante el MPLS *Fast Reroute*, que explicaremos más en detalle en apartados siguientes. Este protocolo además es capaz de detectar fallos tanto unidireccionales como bidireccionales. *{4}*

5.3.4 Contención

Como hemos comentado anteriormente, puesto que la red de transmisión, en algunas ocasiones, entregará un ancho de banda inferior a los enlaces de 1x10GE, el 7750-SR debe estar configurado para limitar dichos enlaces a la capacidad real, adecuando a la vez la calidad de servicio acorde con dicha capacidad. En caso de que el 7750-SR sobrepase esta limitación, los equipos *LambdaUnite* generarán tramas Ethernet 802.3 con un intervalo de pausa hacia el router 7750-SR que, una vez recibidas por este, servirán para que el mismo inhabilite la transmisión durante el periodo de tiempo indicado en las tramas.

Una vez recibidos estas tramas, pese a que durante dicho intervalo de tiempo el router impide la transmisión de datos, los mecanismos de calidad de servicio siguen estando operativos. Por ello, el tráfico *EF (Expedited Forwarding)* será atendido antes que el tráfico *best-effort* o de baja prioridad. En el caso de que el equipo 7750-SR esté recibiendo continuamente este tipo de tramas pausadas, es probable que se llegue al punto de descartar tráfico y teniendo en cuenta que los *buffers* de las colas de tiempo real son considerablemente inferiores a los del tráfico *best-effort,* el tráfico en tiempo real será descartado con más facilidad.

En la siguiente tabla se muestran los intervalos de pausa dependiendo del número de VC4s.

Número de VC4s	Tiempo de pausa (ms)
1xVC4	1,92256
2xVC4	0,458752
3xVC4	0,114688
4xVC4	0,06528
5xVC4	0,031744
6xVC4	0,024064
7xVC4	0,016384

Tabla 13: Intervalos de pausa por VC4

5.3.5 Interfaces de red

Los interfaces de red hacen referencia a todos aquellos interfaces sobre los cuales se va a cursar tráfico. En esta sección se pretende detallar ciertos parámetros generales de dichas interfaces.

5.3.5.1 Unidad máxima de transferencia

Gracias a la utilización de los equipos LambdaUnite, estos son capaces de manejar tramas de tipo *jumbo* por lo que no es necesario limitar la *MTU* en los puertos. Su valor por defecto es de 9212 bytes.

5.3.5.2 802.3ah EFM OAM

Tal y como se ha mencionado en el apartado 3.2.3, se hará uso de este protocolo con el fin de descubrir un fallo en la transmisión y es capaz de detectar un fallo en los enlaces unidireccionales y deshabilitar los puertos origen y destino. Esto proporciona a ISNET una ventaja considerable frente a muchas implementaciones que requieran de detección de fallos bidireccionales y no soporten detección unidireccional.

Puesto que se consideran dos esquemas ante fallo simple, una para ISNET y otra para la parte de transmisión, se dispondrá de dos contadores de 802.3ah, dependiendo de si el fallo está protegido o no (ver tabla esquema protección).

Para el caso de “1+1”, ISNET no tendrá constancia del fallo, ya que la convergencia de transmisión es más rápida que en 802.3ah. La única condición por la que 802.3ah está fijado con contadores inferiores, es con el fin de tener una alternativa para detectar fallos en el caso de que la parte de “1+1” no actúe como debiera.

En la siguiente tabla aparecen los intervalos de tiempo de dichos contadores.

Enlace protegido por	Contador (ms)	Tiempo de convergencia (ms)
Transmisión	150	300
ISNET	600	1600

Tabla 14: Contadores 802.3ah

Para un enlace, ambos puertos deben tener la misma configuración 802.3 ah o si no, los puertos son declarados operativamente como "*down*".

5.3.5.3 Autonegociación

Puesto que todos los puertos dentro de un mismo LAG deben tener la misma velocidad, el parámetro de autonegociación deberá estar habilitado o no en modo imitado, para asegurar que la velocidad determinada está registrada. Por tanto para seguir manteniendo la funcionalidad RDI pero asegurando a la vez la misma velocidad, los puertos de Gigabit Ethernet pertenecientes a un mismo LAG deberán estar configurados en modo de autonegociación limitado.

```
A:XXXPE01# configure port 2/1/1
A:XXXPE01>config>port# ethernet autonegotiate limited
```

Comando 1: Configuración de autonegociación

5.3.5.4 Link Aggregation Groups

Para conexiones entre los routers que cuentan con más de un enlace entre ellos, ya sea de Nx1GB o Nx10GB, se agruparán en lo que denominaremos *Link Aggregation Group* o LAG. Para que varios enlaces estén en un mismo LAG, estos deben tener la misma velocidad, es decir en un LAG no puede haber enlaces con diferente ancho de banda entre ellos. Además los puertos deben estar en modo "*no autonegotiate*" o "*autonegotiate limited*".

Una de las ventajas de configurar LAGs es que el tráfico de todos los enlaces del propio LAG se reparte de manera balanceada, por lo que no habrá una diferencia considerable en el porcentaje de ocupación de cada enlace.

```
A:XXXPE01# configure port 1/2/1
A:XXXPE01>config>port# ethernet autonegotiate limited
A:XXXPE01# configure port 2/2/1
A:XXXPE01>config>port# ethernet autonegotiate limited
A:XXXPE01# configure lag 1
A:XXXPE01>config>port# port 1/2/1
A:XXXPE01>config>port# port 2/2/1
```

Comando 2: Configuración de LAG

Debido a que no se configura LPT en los equipos de transmisión, no hay propagación de fallos por lo que se requiere de un protocolo en el LAG que avise del estado de un puerto caído al puerto del otro extremo para evitar que se envíe tráfico innecesariamente.

Los siguientes protocolos serán de utilidad para este propósito:

- LACP
- 802.3 ah

A pesar de que el protocolo 802.3 ah cuenta con un tiempo de convergencia menor, se recomienda además el protocolo LACP, que supondrá una mayor facilidad a la hora de dar de baja puertos sin que ello afecte al servicio.

Link Aggregation Control Protocol (LACP) proporciona un estándar para el intercambio de información en un enlace que permite al *Link Aggregation Control* alcanzar un acuerdo con la identidad del LAG al cual el enlace pertenece, habilitando así la transmisión y recepción de información.

```
A:MONPE01# configure lag 1
A:MONPE01>config>port# lacp active
A:MONPE01>config>port#
```

Comando 3: Configuración LACP

5.3.5.5 Port-Threshold

Esta función configura el comportamiento de LAG si el número de enlaces operativos es menor o igual a un cierto umbral que denotaremos con el nombre de *port-threshold.*

Puesto que la capacidad de los dos centros contra el Core está provisionada para el 100% de su totalidad, es preferible que se "tire" el LAG (poner en estado "*down")* entero en el momento en que uno de los enlaces caiga, es decir, se configurará el *port-threshold* a un valor de N-1, siendo N el número de interfaces en el LAG.

En cambio la configuración del *port-threshold* para la parte de Internet es algo distinta. La capacidad del LAG nunca debe ser inferior al 50% de la capacidad total.

Dependiendo del número de puertos que tengamos en el LAG, la siguiente tabla muestra el *port-threshold* para cada una de ellos.

Puertos Nx10Gb	Capacidad (Gbps)	Port-Threshold	Porcentaje min LAG
1	10	-	-
2	20	0	50%
3	30	1	67%
4	40	1	50%
5	50	2	60%
6	60	2	50%
7	70	3	57%
8	80	3	50%
9	90	4	56%
10	100	4	50%

Tabla 15: Port-threshold para la parte de Internet

La configuración del parámetro del p*ort-threshold* puede verse en el siguiente comando:

```
A:MONPE01# configure lag 2 port-threshold 1 action down
```

Comando 4: Configuración del Port-threshold

5.3.5.6 Tasa de limitación

Este parámetro configura la tasa de tráfico que pasa por un enlace cuyo ancho de banda se ha decidido limitar. Como se ha mencionado en el apartado 3.2.1 está restricción a nivel de transmisión se llevará a cabo mediante el uso de VC4s. Se ha decidido que cada VC4 dispondrá de 136 Mbps.

Dependiendo del número de VC4s de los que se disponga, se obtendrá una tasa de limitación acorde a ellos. Esto queda reflejado en la siguiente tabla. No obstante, esta limitación solo es válida para determinados números de VC4s y para el caso de enlaces de 10GE.

Número de VC4s	Tasa de limitación
4 VC4	544 Mbps
13 VC4s	1768 Mbps
14 VC4s	1904 Mbps
18 VC4s	2448 Mbps
20 VC4s	2720 Mbps
23 VC4s	3128 Mbps
24 VC4s	3264 Mbps
25 VC4s	3400 Mbps
26 VC4s	3536 Mbps
27 VC4s	3672 Mbps
30 VC4s	4080 Mbps
33 VC4s	4488 Mbps
35 VC4s	4760 Mbps
37 VC4s	5032 Mbps
43 VC4s	5848 Mbps
50 VC4s	6800 Mbps
58 VC4s	7880 Mbps
64 VC4s	8704 Mbps

Tabla 16: Tasa de limitación por VC4

El *egress-rate* se configura de la siguiente forma:

```
A:MONPE01# configure port 1/1/3 ethernet egress-rate 136000
```

Comando 5: Configuración de egress-rate

5.4 DIRECCIONAMIENTO Y NOMBRADO

5.4.1 Direccionamiento

Una de los requisitos en cualquier red privada es la necesidad de definir una serie de direcciones IP privadas. Por tanto, nos basaremos en la RFC1918 para asignar dichas direcciones. Se ha decidido usar los siguientes rangos de direcciones según su destino y función. *{1}*

Subred	Reservado para
10.34.0.0 /24	*Loopbacks*
10.34.0.0-31	*Loopbacks* Core
10.34.0.0-15	Plano superior Core
10.34.0.16-31	Plano inferior Core
10.34.0.32-63	Libre
10.34.0.64-95	Zone A/B
10.34.0.96-127	Libre
10.34.0.128-159	Zone C
10.34.0.160-191	Libre
10.34.0.192-223	Zone D
10.34.0.224-255	Libre

Tabla 17: Direcciones IP

Todas las interfaces deben configurarse incluyendo una máscara /30.

Un ejemplo de cómo asignar una dirección IP se muestra a continuación:

```
A:ALIPE01# configure router interface <if-name>
A:ALIPE01>config>router>if$ address 10.34.0.66/30
A:ALIPE01 >config>router>if$ no shutdown
```

Comando 6: Asignación IP

5.4.2 Nombrado

Puesto que en el apartado anterior hemos decidido la posición donde irán todos los centros, es necesario seguir un criterio a la hora de saber cuál es cuál. Para ellos se seguirá el siguiente formato, por orden de escritura.

- Localización: Las tres primeras letras identificarán el nombre del centro. Ver tabla 18.
- Función: Las dos letras siguientes indicarán el tipo de router, ya sea PP, RR o PE.
- Número: Dos números identificarán si pertenece al plano superior, inferior, internet o si se tratará de un PE externo. Se usarán los números 01, 02, 10 y 11 respectivamente.

En la siguiente tabla se muestra la localización de cada centro.

Centro	Localización
San Sebastián de los Reyes	SSR
Alicante	ALI
Barcelona	BCN
Braga	BRG
Castellón	CST
Coimbra	COI
Córdoba	COR
Granada	GRA
Lisboa	LIS
Málaga	MAL
Moncloa	MON
Móstoles	MOS
Murcia	MUR
Oporto	OPO
Oviedo	OVI
Pamplona	PMP
Plaza Castilla	PLC
Pontevedra	PON
Salamanca	SAL
Sevilla	SEV
Valencia	VAL
Vigo	VIG
Vitoria	VIT
Zaragoza	ZGZ

Tabla 18: Localización por centro

Una vez definidos todos, es importante mencionar que no todos los centros de ISNET tendrán conexión con los 7950 XRS de Internet, es decir, con los SSRPE10 y PEESMOS04. Se ha decidido que 12 de las 24 localizaciones, tendrán conexión directa con los anteriores. A continuación se detallan estos centros:

Site	Localización
Alicante	ALI
Barcelona	BCN
Braga	BRG
Castellón	CST
Córdoba	COR
Málaga	MAL
Moncloa	MON
Oporto	OPO
Oviedo	OVI
Pamplona	PMP
Plaza Castilla	PLZ
Vigo	VIG

Tabla 19: Centros conexión Internet

Además, tres de los seis RRs estarán destinados para la parte de internet, concretamente los SSRRR10, MOSRR10 y VALRR10, tal y como se puede observar en la figura 14.

5.5 PLANO DE CONTROL

El plano de control está compuesto por los protocolos y procedimientos destinados al intercambio de información entre protocolos de nivel 3, estos son:

- Intercambio de información de encaminamiento
- Intercambio de etiquetas

5.5.1 IS-IS

IS-IS, *Intermediate System* to *Intermediate System* es un protocolo de enrutamiento de la capa de red, que permite a sistemas intermedios, ISs, dentro de un mismo dominio, cambiar su configuración e información de *routing* para facilitar la información de encaminamiento y funciones de transmisión de la capa de red.

Al igual que *OSPF (Open Shortest Path First)*, se trata de un protocolo de estado de enlaces, que permite una rápida convergencia además de ser de gran escalabilidad. Está basado, por tanto, en la utilización del Algoritmo de Dijsktra para encontrar el mejor camino a través de la red. Ambos soportan máscaras de subred de diferente longitud, pueden usar *multicast* para encontrar routers vecinos mediante paquetes *hello*, y pueden soportar autenticación de actualizaciones de encaminamiento.

No obstante, existen diferencias importantes en el modo de operación de ambos protocolos, por ejemplo en el modo en el que la dirección de área es asignada. En IS-IS, tanto ésta como la dirección del host son asignadas al router entero, mientras que en OSPF, el direccionamiento es asignado al nivel de interfaz.

5.5.1.1 Funcionamiento

Su funcionamiento consiste en la siguiente forma:

- Los routers que utilizan este tipo de protocolo tal y como hemos mencionado antes, comienzan enviando paquetes de difusión conocidos como *hello* para tener conocimiento del área y descubrir dónde están los nodos vecinos.
- Cada router envían paquetes de tipo LSP (*Label Switched Path*) a todos los vecinos adayecentes menos al vecino del cual se recibió el LSP.
- Los routers crean a partir de dichos LSPs, una base de datos con la información de cada vecino y del estado de enlace entre ellos.
- Cada IS calcula un árbol de camino más corto sobre el cual crea la tabla de rutas.

5.5.1.2 Jerarquía

Entre sus funciones, IS-IS está diseñado específicamente para soportar encaminamiento en grandes dominios en combinación con todo tipo de subredes. Para ello, este protocolo se basa en un enrutamiento intradominio a nivel jerárquico, en el cada dominio puede estar dividido administrativamente en áreas y en el que cada sistema reside en un área. Por tanto, se emplea un nivel jerárquico de dos niveles. El *routing* dentro del área, es conocido como *routing* de nivel 1 mientras que el *routing* de nivel 2 es aquel empleado entre dichas áreas. Aunque cabe destacar, que aparece un tercer tipo de router, conocido como *routing* de nivel 1 y 2.

El primero de ellos solo conoce la topología de su propia área y por tanto solamente contiene información de *routing* de la misma, a pesar de tener vecinos de nivel 1 o de nivel 1 y 2.

Para un paquete cuyo destino es otra área, un IS de nivel 1 envía dicho paquete al IS de nivel 2 más cercano dentro de su propia área, independiente del área de destino. El paquete es enviado mediante el *routing* de nivel 2 al área de destino, dentro de la cual se operará mediante el router del primer nivel.

El segundo de ellos puede no solo tener vecinos dentro de la misma área sino también en otras diferentes. Consecuentemente tiene información de otras áreas pero no tiene ningún conocimiento sobre la topología interior de las mismas.

El router de nivel 1 y 2 puede tener vecinos de cualquier área, por lo que dispone de dos bases de datos, una de nivel 1 para el *routing* interno y una de segundo nivel para el interdominio.

Un esquema de lo visto en los párrafos anteriores se puede apreciar en la siguiente figura.

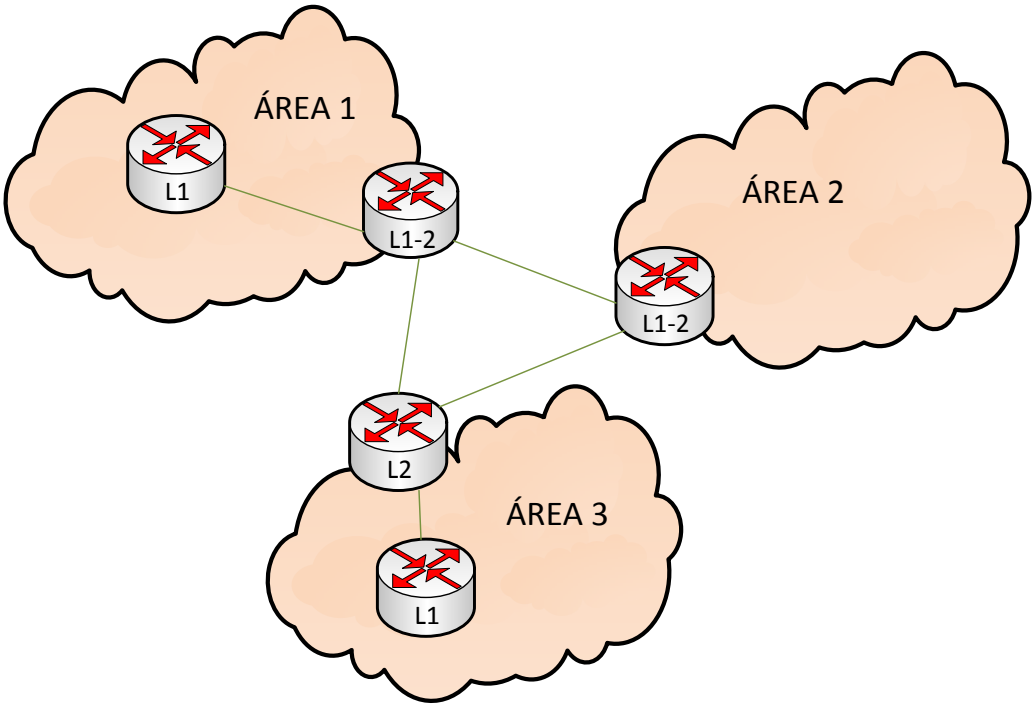


Figura 16: Mapa esquemático de IS-IS

A la hora de facilitar una RSVP-TE *full-mesh* de LSPs entre los PE-Cs, pero evitando el uso de *TE (Traffic Engineering)* entre las áreas, todos los elementos de nuestra red formarán parte de un solo nivel 2. Cada nodo estará además configurado como un IS de nivel 1 y 2 pero cada interfaz hacia el Core funcionará como interfaces de nivel 2.

Echando un vistazo a la parte de configuración, se pueden usar los siguientes comandos:

1. Configuración de un IS nivel 1 y 2.

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# level-capability level-1/2
```

Comando 7: Configuración de un IS nivel 1 y 2

2. Configuración de cada interfaz como nivel 2

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# interface system
A:7750SR>config>router>isis>if# level-capability level-2
```

Comando 8: Configuración nivel 2

5.5.1.3 Convergencia

A la hora de utilizar IS-IS como protocolo de rápida convergencia, es necesario establecer una serie de contadores.

- El intervalo *Shortest Path First* o SPF. Cada IS crea un mapa esquemático mediante el algoritmo de Dijkstra, la cual se calcula a partir del *SPT* (*Shortest Path Tree*). Si la topología del *SPT* cambia, se volverá a ejecutar el SPF para asegurar la ruta más próxima.
- Intervalo de generación de un LSP. Se trata del tiempo que un IS tarda en generar y transmitir un LSP.

Para la creación de un LSP, se han de configurar una serie de parámetros:

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# lsp-wait <lsp-initial-wait> <lsp-
second-wait>
```

Comando 9: Configuración de un LSP

<lsp-initial-wait>: especifica el retardo para la creación de un LSP.

<lsp-second-wait>: especifica el tiempo entre la creación de dos LSPs. Estará fijado a 1 segundo.

5.5.1.4 Métrica

Antes de que cualquier MPLS TE-LSP se configure, IS-IS debe añadir cierto tipo de información sobre el estado y las características de sus enlaces a otros LSRs y esto se

consigue gracias a las extensiones del TE, tales como la disponibilidad del ancho de banda, los grupos de administración, etc.

En el siguiente comando se lleva a cabo la implementación del TE.

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# traffic-engineering
```

Comando 10: Implementación Traffic Engineering

También es necesario que todos los routers sean capaces de soportar dichas extensiones de IS-IS para facilitar el despliegue de TE sobre la red.

Los LSPs basados en RSVP usarán la métrica de TE en lugar de la de IS-IS y los LSP de LDP, se basarán en el camino más corto o *SP* de IS-IS, teniendo en cuenta que la latencia, sobre la cual se centra LDP, representa el papel crucial para los servicios ofrecidos.

Las métricas de IS-IS serán proporcionales a la latencia del enlace. En la siguiente tabla se muestran algunas métricas para cada tipo de enlace.

Origen / Destino	Destino / Origen	Tipo de enlace	Métrica
XXXPE01	XXXPE01	Plano superior de acceso al CORE	interface-delay (msec) * 100
XXXPE02	XXXPE01	Plano inferior de acceso al CORE	interface-delay (msec) * 100
XXXPE01	XXXPE01	Interfaces dentro del CORE	interface-delay (msec) * 100
XXXRR01	XXXPEXX	*Route Reflector* al CORE	100000
XXXPE11	XXXPE01	Interfaces de plano superior con PE-Es	10000
XXXPE11	XXXPE02	Interfaces de plano inferior con PE-Es	10000
XXXPE01	SSRPE10	Plano superior internet	10000 + interface-delay (msec) * 100
XXXPE02	MOSPE10	Plano inferior internet	10000 + interface-delay (msec) * 100
SSRPE10	MOSPE10	Interfaz entre routers de internet	10000 + interface-delay (msec) * 100
XXXRR10	XXXPE10	Interfaz *Route Reflector* - internet	100000
XXXRR10	XXXPEXX	Interfaz *Route Reflector* - PE	100000

Tabla 20: Métrica de IS-IS

Por ejemplo, en el caso de un enlace con latencia de 5 ms, implica una métrica de 5X100, es decir 500. Dicha configuración queda reflejada en el siguiente comando:

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# interface <if-name>
A:7750SR>config>router>isis>if# level 2 metric 500
```

Comando 11: Ejemplo métrica

<if-name>: nombre IP de la interfaz en concreto.

5.5.1.5 Autenticación

El proceso de autenticación de actualizaciones IGP es un parámetro muy a tener en cuenta. La red deber ser capaz de soportar lo que se conoce como autenticación criptográfica (HMAC-MD5) para los LSPs de IS-IS. Sumado a esto, es más que recomendable el uso de autenticación MD5 para el caso de los LSPs de tipo *hello.*

Para la configuración del primero, se deben utilizar los siguientes comandos:

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# authentication-type message-
digest
A:7750SR>config>router>isis# authentication-key
<authentication-key>
```

Comando 12: Autenticación de IS-IS

Donde se debe definir el tipo de autenticación y la clave, con el fin de identificar las PDUs *(Protocol Data Unit)* por los nodos vecinos.

Los siguientes comandos son los necesarios para la configuración de la autenticación de los MD5 de tipo *hello:*

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# interface <if-name>
A:7750SR>config>router>isis>if# hello-authentication-type
message-digest
A:7750SR>config>router>isis>if# hello-authentication-key
<authentication-key>
```

Comando 13: Configuración MD5 hello

5.5.1.6 Intervalos de tiempo

En la siguiente tabla quedan reflejados los intervalos de tiempo para cada uno de los parámetros relativos a la configuración de IS-IS.

Parámetro	Tiempo por defecto	Tiempo de configuración
lsp-pacing-interval	100 ms	100 ms
retransmit interval	5 s	5 s
lsp-lifetime	12000 s	65535 s
spf-wait	10 s / 1 s / 1 s	2 s / 50 ms / 100 ms
lsp-wait	5 s / 0 s / 1 s	8 s / 0 s / 1 s
IS-IS L1 hello interval	9 s	9 s
IS-IS L1 hello multiplier	3	3
IS-IS L2 hello interval	9 s	10 s
IS-IS L2 hello multiplier	3	3

Tabla 21: Intervalos de tiempo de IS-IS

5.5.1.7 Escalabilidad

La siguiente tabla muestra el número máximo de los distintos parámetros de IS-IS.

Parámetro	7750 SR
Máx. número de interfaces	255
Máx. número de adyacencias en un interfaz	84
Máx. número de LSPs	25K
Máx. número de rutas IPv4	250K
Máx. de routers en un nivel	25K
Tiempo de ejecución SPF in 10K rutas	< 1 segundo
Máx. Number of IPv6 routes	15K
Máx. número de adyacencias en IPv6	250
Máx. número de LSPs IPv6	25K
Máx. número de routers IPv6 por nivel	25K

Tabla 22: Escalabilidad de IS-IS

5.5.2 MPLS

Tal y como hemos comentado en el apartado de la introducción, MPLS será el protocolo de transporte en todo la red. Las funciones básicas de MPLS será implementadas por las extensiones de TE. Aparte de seleccionar rutas distintas al camino IGP más corto, gracias al TE, MPLS cuenta con un mecanismo denominado *Fast Reroute* o re-enrutado rápido, formando parte del proceso de protección local, tema que explicaremos más en detalle en apartados siguientes.

Teniendo en cuenta que nuestra red pretende integrar distintos servicios, se ha de recordar, como se comentó en el apartado de 2.4, los dos tipos de servicios, que son los siguientes:

- Tipo 1: Voz y otro tipo de servicios en tiempo real, más sensibles en cuanto al *jitter* o la pérdida de paquetes, por lo que la red debe proporcionar:
    - Diferentes caminos para minimizar el tráfico.
    - Una recuperación rápida en caso de fallo de enlace.
    - Priorización de tráfico de voz para evitar el *jitter*.
- Tipo 2: Servicios de bases de datos, más sensibles a la latencia, pero menos restrictivos en cuanto a la pérdida de paquetes, por lo que la red debe proporcionar:
    - El mejor camino minimizando la latencia.
    - Recuperación de tráfico en caso de fallo de enlace.

Por tanto, en función del tipo de tráfico que se ofrezca, distinguiremos dos tipos de túneles MPLS:

- RSVP: servicios de tipo 1, en el que se hará uso del TE para contar con diferentes caminos y obtener una tiempo de recuperación mínimo, mediante el *Fast Reroute*.
- LDP: servicios de tipo 2, los cuales se basan en los parámetros de métrica de IS-IS proporcionales a la latencia.

5.5.3 RSVP

5.5.3.1 Mallado de LSPs

El mallado de los LSPs TE será desplegado entre todos los PEs, ya sean externos o no. La razón por la que se decide usar este tipo de mallado completo es no solo por la necesidad de despliegue de *Fast Reroute*. RSVP-TE será utilizado para tratar los servicios de primer tipo.

A la hora de activar el protocolo MPLS en una interfaz, también se activará el protocolo RSVP en dicha interfaz.

5.5.3.2 Métrica de TE

Los LSPs basados en RSVP se llevarán a cabo siguiendo la métrica de TE, en lugar de la de IS-IS. Dependiendo del tipo de enlace, los valores acordes con dicho parámetro quedan reflejados en la siguiente tabla.

Origen Destino	Origen Destino	Tipo de enlace	Métrica (ms)
XXXPE01	XXXPE02	Colocalizado	90
XXXPE01	XXXPE01	Plano superior de acceso al CORE	100
XXXPE02	XXXPE01	Plano inferior de acceso al CORE	100
XXXPE01	XXXPE01	Interfaces dentro del CORE	100
XXXPE01	SSRPE10	Plano superior internet	1000
XXXPE02	MOSPE10	Plano inferior internet	1000
SSRPE10	MOSPE10	Interfaz entre routers de internet	1000
RRESXXX01	XXXPE01	*Route Reflector* al CORE	-
XXXRR10	XXXPEXX	Interfaz *Route Reflector* - PE	100000
XXXPE11	XXXPE01	Interfaces de plano superior con PE-Es	200
XXXPE11	XXXPE02	Interfaces de plano inferior con PE-Es	200

Tabla 23: Métrica de TE

Un ejemplo de la configuración de la métrica de un enlace es el siguiente:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# interface <int-name>
A:7750SR>config>router>mpls>if# te-metric 100
```

Comando 14: Configuración métrica TE

<int-name>: nombre del interfaz en cuestión.

5.5.3.3 Colocación y señalización de LSPs

En cuanto a la señalización de TE-LSPs, esta se basa en *Dynamic Constraint-Based routing o DCBR*, el cual proporciona a los PEs TE-LSPs total autonomía para la colocación de los mismos. Éste método de señalización tiene por tanto, el potencial para reducir significativamente el número de horas de programación de los LSPs y además proporciona una mejora en el caso de fallos múltiples.

La configuración de caminos para el RSVP Dinámico será la siguiente:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# path <path-name>
A:7750SR>config>router>mpls>path# no shutdown
```

Comando 15: Configuración RSVP Dinámico

Una vez creado dicho camino, se pasará a la configuración del LSP:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# lsp <lsp-name>
A:7750SR>config>router>mpls>lsp# primary <path-name>
A:7750SR>config>router>mpls>lsp# to <dest. IP address>
```

Comando 16: Configuración de LSP

<lsp-name>: nombre del LSP.

<path-name>: nombre para el camino que se pretende crear.

<dest. IP address>: dirección IP del PE de destino.

También se ha tiene en cuenta los contadores de restablecimiento de LSPs para todos los PEs, con el fin de optimizarlos. Su configuración es la siguiente:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# lsp <lsp-name> retry-timer 5
```

Comando 17: Configuración retry-timer

<retry-timer>: representa el tiempo de espera necesario para la creación del LSP en caso de fallo. Toma el valor de 5 segundos.

Mientras que el DCBR es el modelo establecido por defecto para la protección, es necesario además proporcionar una diversidad de LSPs entre centros con el fin de que se cumplan una serie de requisitos:

- M3UA/*SCTP* resistencia para SIGTRAN, estipula que *multiple single-homed* SCTP y/o *single multi-homed* SCTP no pueden tener en común ningún punto de fallo.
- Bajo condiciones normales, el tráfico entre los PEs debe estar balanceado entre los dos planos.

Para asegurar dicha diversidad de LSPs, se ha decidido el uso de grupos administrativos dentro de MPLS TE. Estos, se van a configurar dependiendo del tipo de enlace.

Tipos de interfaz	Grupo	Comentarios
Plano superior (XXXPE01-XXXPE01)	Superior	Necesario en el lado del PP y opcional en el lado del PE
Plano inferior (XXXPE02-XXXPE01)	Inferior	Necesario en el lado del PP y opcional en el lado del PE
Plano superior CORE	Superior	(VITPP01- LISPP01, VITPP01-SSRPP01,SSRPP01-LISPP01)
Plano inferior CORE	Inferior	(VALPP01-GRAPP01, VALPP01-MOSPP01, MOSPP01-GRAPP01)
Enlaces Core vertical	-	(VITPP01-VALPP01,LISPP01-GRAPP01,SSRPP01-MOSPP01)
Interfaz superior acceso Internet (XXXPE01-SSRPE10)	internet	Solo en el lado del XXXPE01
	Int_sup	En ambos extremos
Interfaz superior acceso Internet (XXXPE02- MOSPE10)	internet	Solo en el lado del XXXPE02
	Int_inf	En ambos extremos

Tabla 24: Tipos de grupos según interfaces

Los grupos administrativos estarán configurados tanto para los 7950-XRS como los 7750-SR (PE-Cs y PE-Es) de la siguiente forma:

Grupo admin	ID
Superior	1
Inferior	2
Internet	3
int_sup	4
int_inf	5

Tabla 25: Administradores

A nivel de comando esto debe ser configurado en todos los routers P y PEs reflejado de la siguiente manera:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# admin-group superior 1
A:7750SR>config>router>mpls# admin-group inferior 2
A:7750SR>config>router>mpls# admin-group internet 3
A:7750SR>config>router>mpls# admin-group int_sup 4
A:7750SR>config>router>mpls# admin-group int_inf 5
```

Comando 18: Configuración admin-group

1) Admin-group *superior* es aplicado a todas las interfaces que se conecten en el plano superior tanto dentro del core entre routers P, como aquellos interfaces entre routers P y PE.

2) Admin-group *inferior*, igual que el anterior pero aplicado al plano inferior.
3) Admin-group *internet* aplicable a todas las interfaces, de ambos planos, que interconecten PEs con los PEs de la parte de Internet, usando la arquitectura relativa a dicha parte. Utilizado para la parte de los PEs.
4) Admin-group *int_sup* es aplicable a todas las interfaces del plano superior con la parte de Internet en ambos extremos.
5) Admin-group *int_inf* igual que el anterior pero el plano inferior.

Sumado a esto, nuestra red contará además con el uso del *ADSPEC*, que servirá para que los datos de aviso estén incluidos en los mensajes RSVP. Gracias a este objeto, los LSPs negociarán la MTU dependiendo de la MTU establecida en al camino LSP.

A nivel de comandos, queda de la siguiente forma:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# lsp <lsp-name> adspec
```

Comando 19: Configuración ADSPEC

Los LSPs de los PEs conectados al plano superior con destino a los PEs del plano inferior deben estar configurados de manera que se evite al plano superior y viceversa.

5.5.3.4 Señalización LSP

Debido a que se usa MPLS-TE como método de protección y no las capacidades del TE, hay un pequeño beneficio en la señalización de LSPs con ancho de banda no nulos o *non-zero*.

5.5.3.5 Prioridades

Cada LSP tiene dos tipos de prioridades, una de *set-up* y otra de *holding* asignadas en el *Session_Attribute* de los mensajes RSVP. La primera de ellas cuenta con ocho niveles, de 0 a 7, siendo el 0 el más prioritario. Este tipo se usa con el fin de decidir si una sesión puede adelantar a otra. La segunda prioridad, con el mismo rango de valores, en cambio su utilidad es para saber si dicha sesión puede ser adelantada por otra.

En el momento que un túnel está establecido, su prioridad de *set-up* es considerada a la hora de decidir si admitir el túnel o no. Cuando se crea otro túnel que compite con el anterior por el ancho de banda, la prioridad de *set-up* del nuevo túnel se compara con la de *holding* del primero de ellos.

Los PE-Cs y los PE-Es señalizarán todos sus LSPs con una prioridad de *set-up* y de *holding* de 7 y de 0 respectivamente, de manera que un LSP nunca puede ser adelantado. Los túneles bypass señalizarán los LSPs con una prioridad de *set-up* y de *holding* de 7.

5.5.3.6 Ancho de banda

El ancho de banda de RSVP se refiere a la capacidad disponible de las reservas de recursos de RSVP por cada enlace MPLS-TE habilitado en la red. Las reservas de ancho de banda *non-zero* para un enlace TE, mencionadas en el apartado anterior, restarán parte del total de la capacidad disponible para otro LSP. Durante el despliegue de la red, se utilizan TE-LSPs de ancho de banda nulos, lo que significa que a la hora de configurar el ancho de banda disponible para cualquier cosa distinta a las interfaces físicas conlleva una capacidad muy pequeña en cuento a TE. Por tanto, lo lógico es que el ancho de banda disponible coincida con el ancho de banda física del puerto.

5.5.3.7 Tiempo de vida y actualización

Existen dos parámetros temporales a tener en cuenta a la hora de mantener un camino RSVP, el periodo de actualización o estado *Resv* y el tiempo de vida local. El primero de ellos se usa para determinar qué valor aplicar para el segundo cuando el estado es recibido y almacenado.

En el caso de aumentar el valor del periodo de actualización, esto supone una mejora en cuanto a la transmisión, pero al mismo tiempo se ve incrementado el tiempo de sincronización de RSVP. Según la RFC2205, este valor se fija a 35 segundos.

A nivel de comandos, para el 7750-SR, se configura de la siguiente forma:

```
A:7750SR>config>router>rsvp# keep-multiplier 3
A:7750SR>config>router>rsvp# refresh-time 35
```

Comando 20: Configuración de keep-multiplier y refresh-time

5.5.3.8 Protocolo Hello

Este protocolo está compuesto por los mensajes de tipo *Hello*, un mensaje de petición más un ACK para la confirmación del anterior. El proceso del mismo está orientado para la comunicación entre dos vecinos, el cual soporta selección independiente de intervalos de detección de fallos. Cada vecino puede automáticamente hacer uso de este tipo de mensajes y en el caso de que el número de *hellos* perdidos sea superior al valor fijado por el *keep-multiplier* (ver comando anterior), este mensaje se considera como perdido.

Como la pérdida de mensajes *hello* no es un condicionante para dar de baja un estado de RSVP, se recomienda la habilitación de *last resort*, para que eso suceda. Para nuestra red el intervalo de *hello* será de 15 segundos con un *keep-multiplier* de 3.

```
A:7750SR#configure router rsvp
A:7750SR>config>router>rsvp# interface system
A:7750SR>config>router>rsvp>if# hello-interval 15000
```

Comando 21: Configuración intervalo hello

5.5.3.9 Reoptimización

La reoptimización es el proceso de la cabecera de un TE-LSP cuando ejecuta un SPF con el fin de encontrar un camino óptimo para un determinado TE-LSP. Supongamos por ejemplo que un TE-LSP ha sido creado mientras que un enlace físico en el camino más óptimo estaba deshabilitado. Obviamente dicho TE-LSP no habría hecho uso de este enlace fallido y sin la reoptimización nunca podría reenrutar sobre el enlace creado al principio.

La gama de modelos 7750-SR y 7950-XRS da soporte a un proceso periódico de reoptimización y se recomienda que este intervalo sea de 30 minutos para cada TE-LSP, por lo que, el LSP será reoptimizado media hora despúes de cuando fue establecido.

Es importante tener constancia de que este proceso no afecta al TE-LSP durante su implementación, es decir, se pueden modificar ciertas características del mismo, tales como el ancho de banda y el camino que el LSP va a tomar, así como que el LSP pueda volver a ser señalizado para evitar pérdida de paquetes. Esto es posible gracias al *Shared-Explicit* o SE RSVP que permite compartir el mismo ancho de banda a dos sesiones para un canal físico determinado.

Desde el punto de vista de la configuración a nivel de comando:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# resignal-timer 30
```

Comando 22: Configuración reoptimización

Pero, es notable tener en cuenta que no es obligatoria la espera de los 30 minutos para la reoptimización. Para ello, se hará uso del siguiente comando:

```
A:7750SR# tools perform router mpls resignal lsp <lsp-name>
path <path-name>
```

Comando 23: Cancelación del intervalo de espera

<lsp-name>: indentificativo del LSP.

<path-name>: identificativo del camino del LSP.

5.5.3.10 Protección

Tal y como mencionamos en el apartado de introducción de MPLS, el mecanismo de *Fast Reroute* forma parte del proceso de restauración y protección configurado en cada enlace de nuestra red. Esta restauración se implementará a través de túneles backup de protección local, también denominados *Bypass Tunnels* para proveer N:1 LSPs de backup, en el que todos los LSPs estarán protegidos. Este proceso es comparable a nivel temporal con SONET/SDH. Estos túneles bypass proporcionarán protección de enlace (NHop) y fallo de nodo (NNHop).

Antes de nada, cabe destacar que se debe activar TE en el IGP, IS-IS en nuestro caso, dentro del mismo área.

```
A:7750SR#configure router isis
A:7750SR>config>router>isis# traffic-engineering
```

Comando 24: Configuración de TE en IS-IS

Fast Reroute

Un punto clave de la protección local es el *PLR (Point of local repair)*, método para detectar fallos. La protección local no facilita directamente dicha habilidad pero se sostiene en mecanismos convencionales tales como SDH/SONET OAM y *keep-alives* de la capa 2. En la parte del Core de la red, donde se usa Ethernet, el detonante dependerá del protocolo 802.3ah. *{4}*

Señalización de túneles *bypass*

Los equipos 7750-SR y 7950-XRS señalizan automáticamente los túneles bypass cuando un LSP primario es señalizado a través del nodo solicitando protección local. Este tipo de túneles son señalizados con anchos de banda nulos para habilitar al menos dos LSPs de backup para compartir ancho de banda en un solo canal físico para protegerlo frente a un fallo simple.

Con el fin de llevar a cabo una estrategia de implementación coherente, un requisito esencial es la necesidad de que los LSPs de backup deben estar conectados pero desde diferentes nodos, a los LSPs primarios, es decir, no deben estar en un grupo en el que compartan riesgo ante fallo. A pesar de que la señalización automática de los túneles bypass no tiene en cuenta estos grupos de riesgo, gracias a la estructura en forma de prisma de la red, esta debe ser capaz de asegurar una diversidad en cuanto a los enlaces o nodos se refiere. No obstante, la misma no es capaz de asegurar una diversidad a nivel de plano de control.

A nivel de comandos, esto queda reflejado de la siguiente forma:

```
A:7750SR#configure router mpls
A:7750SR>config>router>mpls# lsp <lsp-name>
A:7750SR>config>router>mpls>lsp# cspf
A:7750SR>config>router>mpls>lsp# fast-reroute <facility>
A:7750SR>config>router>mpls>lsp>frr# node-protect
```

Comando 25: Configuración fast-reroute

<facility>: este método toma ventaja de las pila de etiquetas de MPLS. En lugar de crear un LSP alternativo para cada LSP de *backup*, solamente se crea un único LSP que servirá de *backup* para un conjunto de LSPs.

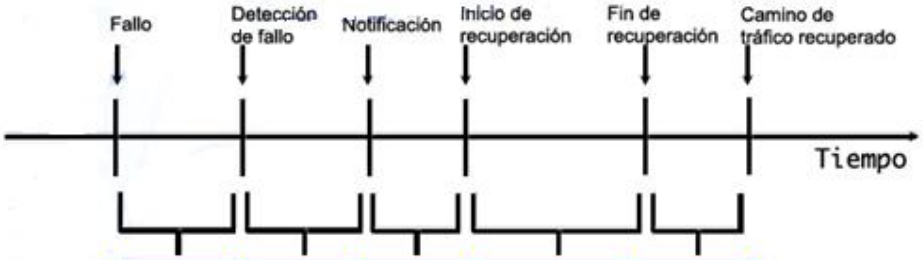
node-protect: este comando brinda la posibilidad de decidir si activar o desactivar la protección del nodo. Dicha protección asegura que el tráfico de un LSP atravesando el router vecino alcanzará el destino independientemente de si el nodo vecino fallo o no. Esta configuración viene impuesta implícitamente en los 7750-SR y 7950-XRS.

Revirtiendo de túneles *bypass* de protección

Durante el periodo en el que un LSP primario es llevado por un túnel de bypass, no tiene lugar ningún tipo de protección, ya que no se puede proteger un túnel de bypass con otro de la misma índole. Por tanto, es un requisito que el LSP se optimice fuera del túnel bypass tan pronto como sea posible.

En *Fast Reroute* Global de modo reversible, cuando un *PLR* sirve de protección para un LSP primario encaminando tráfico por un túnel bypass, señaliza un mensaje de tipo RSVP *PATH-ERROR* a la cabecera del LSP para notificar que el mismo ha sido protegido. La cabecera esperará al intervalo definido en el *Retry-Timer,* (ver apartado 4.2.3) cuyo valor será de 5 segundos para nuestra red, antes de reoptimizar el LSP primario y reorientarlo fuera del túnel bypass. Si existe un camino más óptimo, la cabecera señaliza un nuevo LSP y migra tráfico al mismo. En el caso de que no exista un camino más óptimo, el LSP permanecerá en el túnel bypass y se reoptimizará una vez haya pasado el tiempo de expiración de 30 minutos.

En la siguiente figura podemos ver una comparativa de los tiempos de recuperación y detección de fallo de las diferentes tecnologías frente a *Fast Reroute*, ya sea MPLS local o global.



	Tiempo de detección	Tiempo de Hold-off	Tiempo de notificación	Tiempo de operación de recuperación	Tiempo de recuperación de tráfico
SDH	Microsec – ms	10-20ms	10ms/hop	~10ms	microsec
IP-OSPF	Microsec – ms	10-20ms	10ms/hop	~1-3sec	ms
IP-BGP	Microsec – ms	10-20ms	10ms/hop	~1-15min	ms
MPLS global	Microsec – ms	10-20ms	10ms/hop	5-10 sec	ms
MPLS local	Microsec – ms	10-20ms	10ms/hop	10-50ms	ms

Figura 17: Intervalos de tiempo para las distintas tecnologías

5.5.3.11 LSPs punto-multipunto

Para el transporte de tráfico *multicast* de corporativa como tráfico MPLS en una M-VPN, será necesario túneles de transporte de tipo P2MP (*point to multipoint*). Estos túneles pueden estar basados según mLDP o RSVP-TE, aunque para el *multicast* de la parte corporativa emplearemos túneles de tipo P2MP RSVP-TE LSP.

Un LSP P2MP de tipo RSVP permite al origen del tráfico de *multicast*, encaminar paquetes a uno o más destinatarios sobre una red que no necesariamente tiene porque basarse en un protocolo *multicast*, como es el caso de *PIM* , cuya configuración será obligatoria para la parte del Core.

Un árbol LSP P2MP es creado en el plano de control cuyo camino consiste en un nodo cabecera, uno o más nodos por rama, y los nodos finales, también conocidos como nodos hoja. Los paquetes entregados por el nodo cabecera, serán replicados en el plano de control a cada rama previamente a ser entregados a los nodos hoja.

Un LSP P2MP es un LSP unidireccional que inserta paquetes a la raíz (*ingress* LER) y reenvía exactamente la misma réplica del paquete a uno o más nodos hoja (*egress* LER). El paquete puede ser replicado a la raíz del árbol y/o a otro LSR que actúe como nodo rama.

En la figura posterior, podemos ver la topología en forma de árbol con los distintos tipos de LSR para un dominio MPLS.

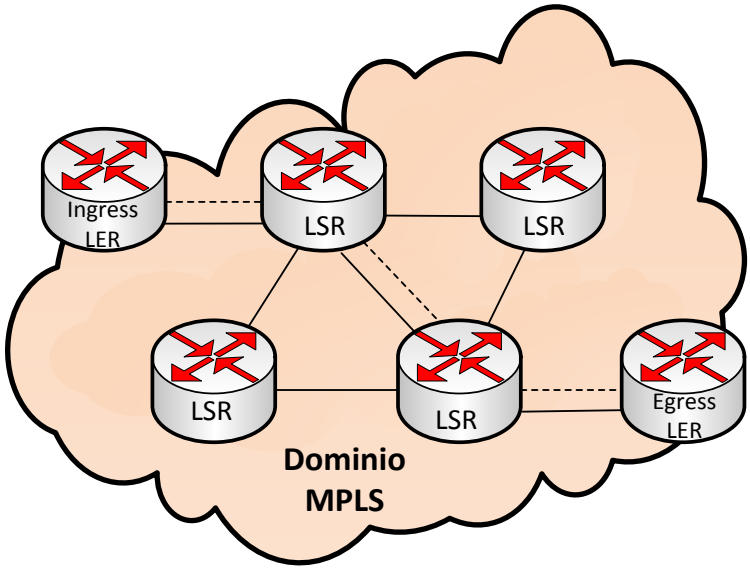


Figura 18: Topología P2MP

Este modelo P2MP será creado en todos los PEs con las siguientes características:

- No se aplicará ninguna restricción en cuanto a los caminos.
- Se habilitará *CSPF*.
- Se empleará *Fast Reroute*.
- Se utilizará un *retry-timer* de 5 segundos para los LSPs de tipo *unicast*, mientras que para el resto se fijará un valor de 30 segundos por defecto.

En la siguiente tabla, se muestra la escalabilidad en lo relativo a P2MP

DSCP	Forwarding Class
P2MP RSVP	200 nodos hoja
Máx P2MP RSVP punto finales	min: 1K, máx: 4K
Árboles P2MP RSVP	20

Tabla 26: Escalabilidad de P2MP

Habrá por tanto, un nuevo camino usado para el LSP P2MP:

```
configure router mpls
   path "mvpn_dyn"
     no shutdown
   exit
exit
```

Comando 26: Asignación LSP P2MP

Una vez que el modelo de P2MP está creado, tiene que estar asociado en la *mvpn* de la VPRN *multicast* bajo el comando *"provider-tunnel".*

5.5.4 LDP

LDP debe ser activado en cada una de los interfaces de la red para que esta funcione.

En caso de fallo de conectividad y su consecuente recuperación entre dos nodos, IGP (ISIS) puede converger antes de que se negocien nuevas etiquetas LDP de trasporte. Ello implica que parte del tráfico al destino sea descartado porque la ruta es correctamente actualizada en la tabla de rutas pero las etiquetas LDP de transporte no están disponibles.

Para evitar la situación anterior, se activará sincronización entre LDP e IGP (ISIS). Para ello, se configurará un contador, *ldp-sync-timer*, que tendrá un valor de 15 segundos. Este contador implica que durante ese intervalo de tiempo, la ruta es anunciada con una métrica infinita, por lo que no será usada y las etiquetas LDP de transporte dispondrán de tiempo suficiente para la negociación.

Puesto que LDP seguirá el camino óptimo de IGP y teniendo en cuenta que las interfaces de los RRs no estarán incluidas en LDP, hay un riesgo entre ISIS y LDP en el caso de que el primero de ellos afirme que las interfaces del RR sean el mejor camino para una FEC determinada y el segundo de ellos diga que es otro camino. En tal caso, el túnel LDP para ese FEC no se establece. Para evitar eso, la métrica de ISIS para los interfaces de los RRs será mucho mayor comparado con el resto de interfaces de la red, como queda reflejado en la tabla 20.

A nivel de comando, el *ldp-sync-timer* queda configurado de la siguiente manera:

```
A:XXXPE01# configure router
        interface "port-5/1/1"
            ldp-sync-timer 15
        exit
        interface "port-lag-1"
            ldp-sync-timer 15
        exit
        interface "port-lag-23"
            ldp-sync-timer 15
        exit
```

Comando 27: Configuración ldp-sync-timer

5.5.4.1 Mallado de LSPs

Sabiendo que LDP funciona como *full-mesh* o mallado completo en su naturaleza, se ha de tener en cuenta los siguientes parámetros en cuanto a su escalabilidad.

Parámetro	R8.0	R9.0	R10.0	R12.0
Máx FECs por *ingress*-LER	16k	128k	128k	128k
Máx FECs por LSR	32k	238k	238k	238k
Máx FECs por *egress*-LER	128k	238k	238k	238k

Tabla 27: Escalabilidad de LSPs de LDP

Para nuestra red, todos los PEs pueden necesitar estos LSPs, por lo que se configurará basándose en *full-mesh.* Su configuración por tanto queda:

```
A:XXXPE01# configure router
        ldp
            tunnel-down-damp-time 0
            interface-parameters
                interface "port-lag-1"
                exit
                interface "port-5/1/1"
                exit
                interface "port-lag-23"
                exit
            exit
        exit
```

Comando 28: Configuración LSPs en PE

<tunnel-down-damp-time>: este comando se usa para especificar el intervalo de tiempo, en segundos, que un LDP espera antes de dar de baja un túnel en el *Tunnel Table Manager (TTM)*.

5.5.5 Configuración general de MPLS

Una vez vistos todos los parámetros de configuración necesarios para MPLS, observemos un ejemplo a nivel de comando en el que se incluyen todos en conjunto.

```
A:XXXPE01# configure
        mpls
            resignal-timer 30
            admin-group "int_inf" 5
            admin-group "int_sup" 4
            admin-group "inferior" 2
            admin-group "internet" 3
            admin-group "superior" 1
            exit
            interface "port-lag-1"
                te-metric 90
            exit
            interface "port-3/1/1"
                te-metric 200
            exit
```

```
            interface "port-lag-28"
                admin-group "int_sup"
                admin-group "internet"
                te-metric 500
            exit
        exit
        rsvp
                hello-interval 10000
            exit
            interface "port-lag-1"
                hello-interval 10000
            exit
            interface "port-3/1/1"
                hello-interval 10000
            exit
            interface "port-lag-28"
                hello-interval 10000
            exit
            no shutdown
        exit
        mpls
            path "dyn"
                no shutdown
            exit
            lsp "P0:XXXPE01:XXXPE01"
                to 10.34.0.24
                cspf use-te-metric
                adspec
                fast-reroute facility
                exit
                retry-timer 5
                primary "dyn"
                exit
                no shutdown
            exit
            lsp "P0:XXXPE01:XXXPE02"
                to 10.34.0.25
                cspf use-te-metric
                adspec
                fast-reroute facility
                exit
                retry-timer 5
                primary "dyn"
                    exclude "internet"
                    exclude "superior"
                exit
                no shutdown
            exit
```

Comando 29: Configuración general de MPLS

5.5.6 Intervalos de tiempo de MPLS

En la siguiente tabla podemos observar los intervalos de tiempo para cada parámetro.

Parámetro	Por defecto	Configurado
LDP Sync Timer	deshabilitado	15 s
Resignal timer	deshabilitado	30 min
LSP retry timer	30 s	5 s
LSP retry limit	0 (siempre)	0 (siempre)
RSVP hello interval	3 s	10 s
RSVP keep multiplier	3	3
RSVP refresh time	35 s	35 s

Tabla 28: Intervalos de tiempo de MPLS

5.5.7 BGP

Nuestra red puede ser considerada como un Sistema Autónomo cuyo propósito es el de crear servicios de tipo BGP y MPLS IP-VPN. {5}

Un Sistema Autónomo o AS, se define como un grupo de redes IP que poseen una política de rutas propia e independiente. Además realiza su propia gestión de tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. A cada AS se le asigna un único número identificativo, que lo distingue frente al resto. Para nuestra red dicho número será el 29992.

```
A:7750SR# configure router
A:7750SR>config>router# autonomous-system 29992
```

Comando 30: Definición Sistema Autónomo

Además de definir dicho número, es necesario también asignar un identificativo del router BGP o uno global antes de configurar ninguno de los *peerings* BGP. En el caso de que ningún identificativo BGP sea determinado, será usado el ID global. Pero si ninguno de los dos es fijado, se usará la dirección IP del sistema, por lo que se recomienda que se configuren ambos con el mismo identificativo. Si, tanto el ID Global como el BGP se configuran, el último de ellos será el usado para el protocolo BGP.

Para definir un ID global:

```
A:7750SR#configure router
A:7750SR>config>router# router-id <IP-address>
```

Comando 31: Definición ID global

Para definir un ID BGP:

```
A:7750SR#configure router bgp
A:7750SR>config>router>bgp# router-id <IP-address>
```

Comando 32: Definición ID BGP

<IP-address>: expresa la dirección IP en notación decimal.

5.5.7.1 Peerings

Tal y como hemos visto en los apartados anteriores, nuestra red dispondrá de tres *Route Reflectors* para la distribución de las VPN-IPv4 y VPN-IPv6. Cada PE-C y PE-E establecerá una sesión iBGP para cada RR y será un cliente de cada uno de ellos. Los tres RRs formarán parte de un único *cluster*.

Los comandos de configuración para una sesión iBGP para un PE hacia un RR son:

```
A:7750SR#configure router bgp
A:7750SR>config>router>bgp# group <group-name>
A:7750SR>config>router>bgp>group# type internal
A:7750SR>config>router>bgp>group# neighbor <neighbor-
address>
A:7750SR>config>router>bgp>group >neighbor# family vpn-ipv4
vpn-ipv6 mvpn-ipv4
```

Comando 33: Configuración iBGP entre PE y RR

Los comandos para una misma sesión iBGP para un RR hacia un PE son:

```
A:7750SR#configure router bgp
A:7750SR>config>router>bgp# cluster 1.1.1.1
A:7750SR>config>router>bgp# group <group-name>
A:7750SR>config>router>bgp>group# family vpn-ipv4 vpn-ipv6
mvpn-ipv4
A:7750SR>config>router>bgp>group# type internal
A:7750SR>config>router>bgp>group# neighbor <neighbor-
address>
```

Comando 34: Configuración iBGP entre RR y PE

<group-name>: nombre del grupo.

<neighbor-address>: dirección IP del router BGP.

En esta última configuración, cabe destacar el identificativo del cluster. Puesto que no queremos subdividir nuestro AS en AS's más pequeños, se usará el mismo ID para los tres RRs.

5.5.7.2 BGP Tracking

El *tracking* o seguimiento, de BGP, proporciona la capacidad de sustraer prefijos VPN-IPv4 de una *VRF* si una dirección IP es eliminada de la topología de IS-IS. Sin esto, y en caso de fallo, los PEs dependerían del *hold timer*¸un contador de espera, entre el PE fallido y el RR con el fin de detectar dicho fallo.

En otras palabras, cuando el interfaz de algún RR falla, la base de datos de *routing* (BGP-RIB) en los PE-Cs se borrará mucho más eficientemente.

A nivel de configuración de comandos:

```
A:XXXPE01# configure router bgp
A:XXXPE01>config>router>bgp# enable-peer-tracking
```

Comando 35: Configuración BGP Tracking

5.5.7.3 Autenticación

Al igual que en IS-IS, para la parte de MPLS también debe haber un proceso de autenticación. Se ha optado por usar el TCP MD5, como método de autenticación criptográfica, definida en la RFC2385 para las sesiones de tipo iBGP y eBGP (*external* BGP*)*. Este tipo de autenticación, a diferencia de IS-IS, define una opción TCP ya que BGP usa TCP para la parte de transporte, pero se ha de diferenciar entre las sesiones iBGP y eBGP.

Puesto que la autenticación se establece entre los routers vecinos, ésta se hace en el nivel del vecino.

A la hora de configurar dicha autenticación para las sesiones iBGP, se han de introducir los siguientes comandos:

```
A:7750SR#configure router bgp
A:7750SR>config>router>bgp# group <name>
A:7750SR>config>router>bgp>group# neighbor <IP address>
A:7750SR>config>router>bgp>group>neighbor# authentication-
key <authentication-key>
```

Comando 36: Configuración Autenticación iBGP

<authentication-key>: una clave para identificar la autenticación. Para un nodo del PE o del RR deber ser la misma en el nivel del vecino. Se optará por el nombre común *isc_bgp.*

5.5.7.4 Min-route-advertisement

Este comando configura el intervalo mínimo para el cual un prefijo puede ser anunciado para un peer. Este parámetro puede ser fijado en tres niveles, global, grupo o a nivel de vecino, y su valor será de 3 segundos.

Para un RR o un PE de la gama de los 7750-SR, su configuración será la siguiente:

```
configure router bgp
config>router>bgp# group "internal"
config>router>bgp>group# min-route-advertisement 3
```

Comando 37: Configuración Min-route-advertisement

Para la parte de Internet, en cambio:

```
configure router bgp
config>router>bgp# group "Internet"
config>router>bgp>group# min-route-advertisement 3
```

Comando 38: Configuración Min-route-advertisement Internet

5.5.7.5 Configuración Min-route-advertisement

Puesto que para BGP, la configuración es diferente entre los RRs y los PEs, ya sean 7750-SR o 7950-XRS distinguiremos dos tipos.

Para el primero de ellos:

```
A:XXXRR01# configure router bgp
A:XXXRR01>config>router>bgp# info
----------------------------------------------
            cluster 1.1.1.1
                extended-community
                    accept-orf
                exit
            exit
            group "internal"
                family vpn-ipv4
                authentication-key isc_bgp
                min-route-advertisement 3
                type internal
                neighbor 10.34.0.67
                exit
                neighbor 10.34.0.68
                exit
                neighbor 10.34.0.129
            exit
```

Comando 39: Configuración BGP RR

Para el caso de los PEs 7750-SR:

```
A:7750SR#>config>router>bgp# info
----------------------------------------------
            enable-peer-tracking
                extended-community
                    send-orf
                exit
            exit
            group "internal"
                family vpn-ipv4
                authentication-key isc_bgp
                min-route-advertisement 3
                type internal
                neighbor 10.34.0.7
                exit
                neighbor 10.34.0.8
                exit
                neighbor 10.34.0.20
                exit
            exit
```

Comando 40: Configuración BGP 7750SR

Para la parte de Internet:

```
A:7950XRS#:>config>router>bgp# info
----------------------------------------------
            group "Internet"
                family vpn-ipv4
                authentication-key isc_bgp
                min-route-advertisement 3
                type internal
                neighbor 10.34.0.87
                  description "Sesion BGP con XXXRR10"
                  family vpn-ipv4 vpn-ipv6
                exit
                neighbor 10.34.0.89
                  description "Sesion BGP con XXXRR10"
                  family vpn-ipv4 vpn-ipv6
                exit
                neighbor 10.34.0.148
                  description "Sesion BGP con XXXRR10"
                  family vpn-ipv4 vpn-ipv6
                exit
            exit
```

Comando 41: Configuración BGP 7950 XRS

5.5.7.6 Intervalos de tiempo

Parámetro	Por defecto	Configurado
min-route-advertisement	30 s	3 s(PE)/ 3 s (RR)
connect-retry	120 s	120 s
hold-time	100 s	100 s
Keep-alive	35 s	35 s

Tabla 29: Intervalos de tiempo BGP

5.6- Calidad de Servicio - QoS

QoS o calidad de servicio, es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente, mide la calidad de los servicios dentro de la red, como el ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, pérdida de paquetes o *jitter*, entre otros.

Lo ideal sería que todas las aplicaciones o en nuestro caso, toda la red, gozara de una disponibilidad de recurso de ancho de banda y CPU infinitas, pero desgraciadamente este tipo de recursos son costosos y la asignación de ambos supone un precio muy elevado para los *Proveedores de Servicios* o *ISPs*.

Por tanto, dichos recursos tienen que ser gestionados con el fin de garantizar un rendimiento mínimo para los servicios. Pero se ha de tener en cuenta también, que las garantías no son las mismas ni para cada *flujo* o usuario, ni para el coste por el mismo.

Para ello, se deberá diferenciar, dependiendo del servicio ofrecido, una QoS distinta. Por ejemplo, en aquellas aplicaciones las cuales sean menos tolerantes a retardos, como es el caso de VoIP, se establecerán unas políticas de QoS más restrictivas.

Según la IETF, *Internet Engineering Task Force*, se distinguen dos tipos de servicios, IntServ y DiffServ.

El primero de ellos, también conocido como RSVP (Resource Reservation Protocol) se basa en un modelo de reserva de recursos por flujo durante todo el camino que siguen los paquetes de dicho flujo. Un flujo queda identificado por la dirección IP origen y destino, el protocolo a nivel de transporte y opcionalmente el puerto destino. La aplicación es responsable de gestionar la reserva de recursos en la red y garantizar la obtención de cierta QoS.

En el segundo de ellos, los paquetes se marcan a la entrada de la red DiffServ y dependiendo de las categorías o clases, se establecen distintos parámetros de QoS. En una misma clase se agregan diferentes flujos que se les otorgará el mismo tratamiento de QoS.

5.6.1 Clases de Servicios

En el caso de nuestra arquitectura propuesta y de nuestra red, la QoS estará basada en un modelo de DiffServ en el que cada clase de tráfico (DSCP) está asociado a un comportamiento por salto, PHB (Per Hop Behaviour). Dicho PHB determina el tipo de tratamiento que se le va a dar al paquete en el reenvío.

Dependiendo del tipo de servicio, se distinguen los siguientes grupos de PHB asociados al campo DSCP:

- EF (Expedited Forwarding): DSCP=101110. Bajas pérdidas, baja latencia, bajo jitter, similar a una línea de datos alquilada.
- VA (Voice Admit): DSCP=101100 Similar a EF que añade un mecanismo de control de admisión de llamadas.
- AF (Assured Forwarding): Se proporciona cierta garantía de entrega siempre y cuando se cumpla el acuerdo entre cliente y proveedor sobre el tráfico enviado. Se diferencian cuatro clases, AF4, AF3, AF2 y AF1, siendo AF4 y AF1 la más y menos prioritaria respectivamente.
- DF (Default Group): DSCP=000000. IP *Best Effort*, compatible con tráfico que no es DiffServ.
- CS (Class Selector): usa los 3 primeros bits DSCP=XXX000 para definir prioridades.

En la siguiente tabla se muestran las distintas aplicaciones dentro de nuestra red, seguidas de la clase de servicio y su DSCP asociado.

Aplicación	Ejemplo	Clase de Servicio	DSCP
Protocolo de Control	RSVP, BGP	Control	CS-6
3GPP señalización	Iu-CS, Iu-PS	Señalización	AF41
SIGTRAN	-	Señalización	AF41
3GPP conversacional, VoIP, VoATM	Voz, videoconferencia	Tiempo real	EF
3GPP y TCP Streaming	Audio/Video-*streaming*	Datos críticos	AF42
Aplicaciones críticas de negocios		Datos críticos	CS3

3GPP Interactivo 1	Servicios interactivos de alta prioridad	Datos críticos	AF31, AF32, AF33
3GPP Interactivo 2	Servicios interactivos de prioridad media	Datos críticos	AF21, AF22, AF23
3GPP Interactivo 3	Servicios interactivos de baja prioridad	Datos críticos	AF11, AF12, AF13
Tráfico Móvil de Internet	-	Estándar	Default
Tráfico Fijo de Internet, usuarios Corporativa	-	Best effor	BE

Tabla 30: QoS Clases de Servicio

El marcado de la QoS, la *Forwarding Class* y el tipo de colas que garantizan las clases de servicio descritas en la tabla anterior, quedan detallados en la tabla que aparece a continuación. La columna con el nombre de WRED, representa un mecanismo que permite manejar niveles de descarte de paquetes que explicaremos posteriormente en este apartado.

Clase de Servicio	Forwarding Class	Tipo de Servicio	WRED
CONTROL	Control de Red	Alta Prioridad	No
TIEMPO REAL	EF	Alta Prioridad	No
SEÑALIZACIÓN	Alta-1	Alta Prioridad	No
DATOS CRÍTICOS	Baja-1	*Best Effort*	Yes
	AF		
ESTANDARD	Baja-2	*Best Effort*	No
BEST EFFORT	*Best effort*	*Best Effort*	No

Tabla 31: QoS Diffserv

De acuerdo al diseño de la red, se han establecido unos parámetros rigurosos en cuanto a la QoS se refiere, dependiendo del tipo de tráfico.

Tráfico	Retardo promedio	Retardo máximo	Jitter	Pérdida de paquetes
CS-plano de usuario	< 20ms	< 125ms	< 7ms	< 100-4
Señalización	< 20ms	< 125ms	N/A	< 100-4

Tabla 32: Requisitos SLA

5.6.2 Política de colas a nivel de red

La política de colas a nivel de red o *Network Queue,* define la planificación de las características para cada Forwarding Class, tales como el ancho de banda o el buffer.

Las siguientes tablas representan el porcentaje *CIR/PIR*, *MBS* y *CBS* para cada una de las *network queues* y el máximo retardo para cada cola.

Enlaces en el CORE								
FC	**Cola**	**Descripción**	**PIR**	**CIR**	**MBS (ms)**	**CBS (ms)**	**Prioridad**	**Tipo de tráfico**
BE	1	Best effort	100	5	100	1	Prioridad baja	Corporate backup-usuarios + Regional Fijo Internet
L2	2	Estándar	100	15	100	1	Prioridad baja	Regional Movil Internet + usuarios de corporativa
AF	3	Datos críticos	100	65	75	10	Prioridad baja	VPNs + interfaces 3GPP + Resto de Servicios Corporativos
L1	4	Datos en tiempo real (Video)	100	15	5	5	Prioridad baja	-
EF	6	Voz	70	70	5	5	Prioridad alta	Voz fija y móvil
H1	7	Sigtran	100	20	10	10	Prioridad alta	Señalización
NC	8	Control	100	10	10	10	Prioridad alta	Control

Tabla 33: Tipo de cola and CIR/PIR para el Core

Para la parte de Internet, queda definido en la siguiente tabla.

INTERNET LINKS								
FC	**Cola**	**Descripción**	**PIR**	**CIR**	**MBS (ms)**	**CBS (ms)**	**Prioridad**	**Tipo de Tráfico**
BE	1	Best effort	100	40	100	1	Prioridad baja	Internet Fijo
L2	2	Estándar	100	60	100	1	Prioridad baja	Internet Móvil
AF	3	Datos críticos	100	0	75	10	Prioridad baja	-
L1	4	Datos en tiempo real (Video)	100	0	5	5	Prioridad baja	-
EF	6	Voz	70	70	5	5	Prioridad alta	-
H1	7	Sigtran	100	20	10	10	Prioridad alta	-
NC	8	Control	100	10	10	10	Prioridad alta	-

Tabla 34: Tipo de Cola y CIR/PIR para la parte de Internet

5.6.3 WRED

WRED, *Weighted random early detection*, es un mecanismo de gestión de colas apropiado para evitar congestión. Es una extensión de RED, *Random early detection*, en el que una cola puede tener diferentes umbrales de descarte de paquetes, asociados a una determinada clase de tráfico, dependiendo de lo prioritario que sean dichas clases.

Este modelo se basa en el descarte de paquetes con una probabilidad que depende del tamaño medio de la cola.

En el caso de nuestra red, la política de WRED solo será aplicable a los 7750-SR, los cuales contarán con dos perfiles WRED, aplicados al espacio de buffer compartido. Para cada buffer habrá dos pendientes, *low slope* y *high slope.* La primera de ellas, se encarga de gestionar el acceso al buffer compartido del tráfico de la cola de menor prioridad, mientras que la de mayor prioridad es tramitada por la segunda de ellas. La combinación de ambas, permite que al tráfico de mayor prioridad se le asigne un mayor peso, proceso conocido como *Weighted* RED, de ahí su nombre. Por defecto, sendas pendientes están deshabilitadas y los paquetes son descartados en una cola. Esto se puede contemplar en la siguiente figura. *{10}*

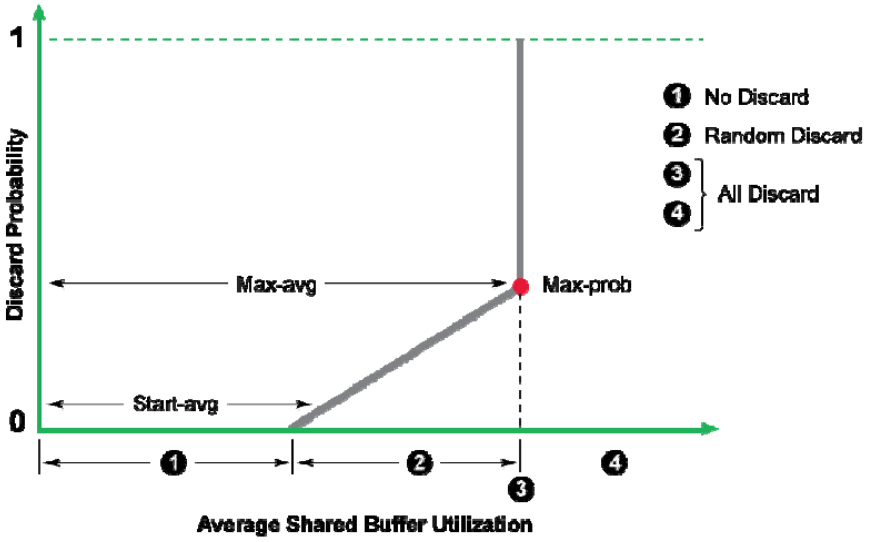


Figura 19: Parámetros WRED

La probabilidad de descarte viene impuesta según los parámetros que aparecen en la figura anterior.

- *Start-avg*: en el que la probabilidad de descarte comienza a partir de cero.
- *Máx-avg*: en el que la probabilidad de descarte crece hasta alcanzar el máximo valor.
- *Máx-prob*: define la pendiente entre el *Start-avg* y el *Máx-avg.*
  Se distinguen por tanto, cuatro regiones:
- *<(0,0) a (start-avg,0)>:* cuando la utilización del buffer está entre cero y *Start-avg.*, la probabilidad de descarte es nula, por lo que no hay pérdida de paquetes.
- *<(start-avg,0)>: a (Máx-avg, Máx-prob>:* cuando está entre *start-avg* y *Máx-avg.*, la probabilidad de descarte es proporcional a la media utilizada por el buffer y oscila entre cero y *Máx-prob.* Para cada paquete, un número aleatorio entre 0 y 1 es asignado. En el caso de que dicho número esté por encima de la curva, el paquete es aceptado. En caso contrario se descartará el paquete.
- *<(Máx-avg, Máx-prob) a (Máx-avg, 1>:* En el umbral de *Máx-avg*, la probabilidad de descarte crece directamente a 1.
- *<(Máx-avg, 1) a (100%, 1>:* la probabilidad de descarte es 1, por lo que todo paquete que llegue será descartado.

Una vez que la cola sobrepasa su reserva de buffer y empieza a usar buffers compartidos, cada paquete es tratado según este modelo.

Además, aparece otro factor en escena, TAF (*Time Average Factor)*, que define la respuesta de la función WRED. Un TAF bajo implica que dicha función actúa

rápidamente frente a los cambios de buffer y viceversa. El TAF permite a la red el paso de ráfagas transitorias de tráfico sin que WRED sea activado. El requisito para que las ráfagas tengan un alto TAF está relacionado con la congestión, la cual es más probable que ocurra cuando el tráfico es *Fast Reroute*.

5.6.4 Scheduler

El *scheduling* o planificación, determina cuando encaminar un paquete a una cola específica, ya sea dentro o fuera de otro router. El *scheduler* dependerá del tipo de tarjeta a la que pertenezca, ya sea IOM2, IOM3 o IMM.

Las siguientes figuras muestran el comportamiento del *scheduler* para cada tarjeta.

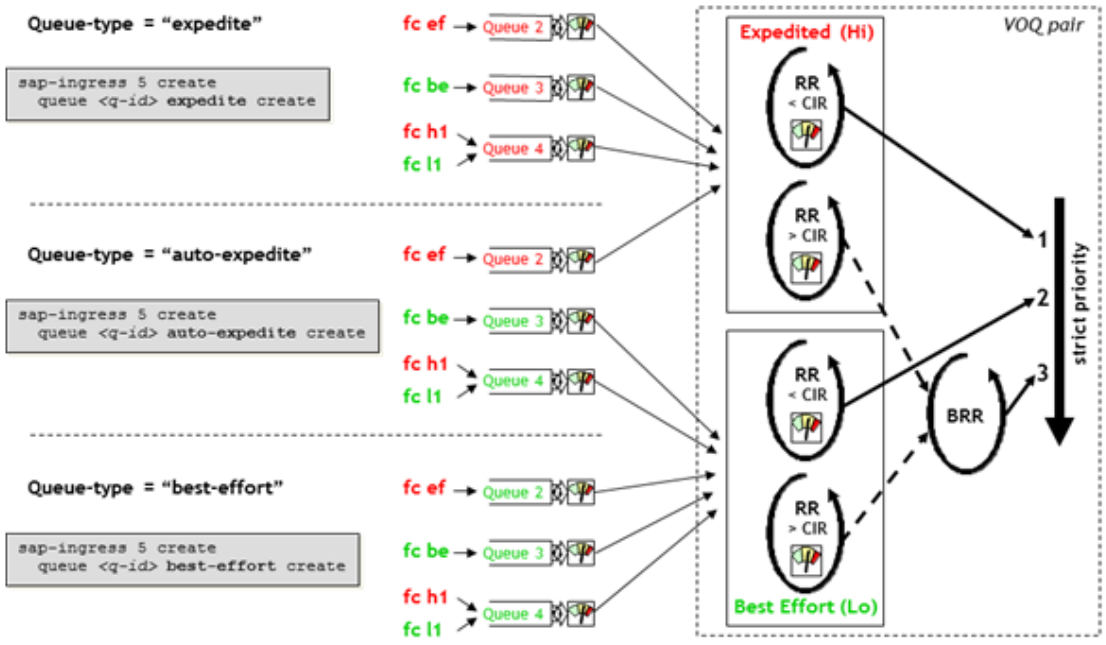


Figura 20: IOM2 Scheduler

Implementa tres tipos de prioridad, en la que la prioridad alta por debajo del CIR es la primera atendida, seguida de la baja prioridad por debajo de la CIR y por último la alta y baja prioridad por encima del CIR.

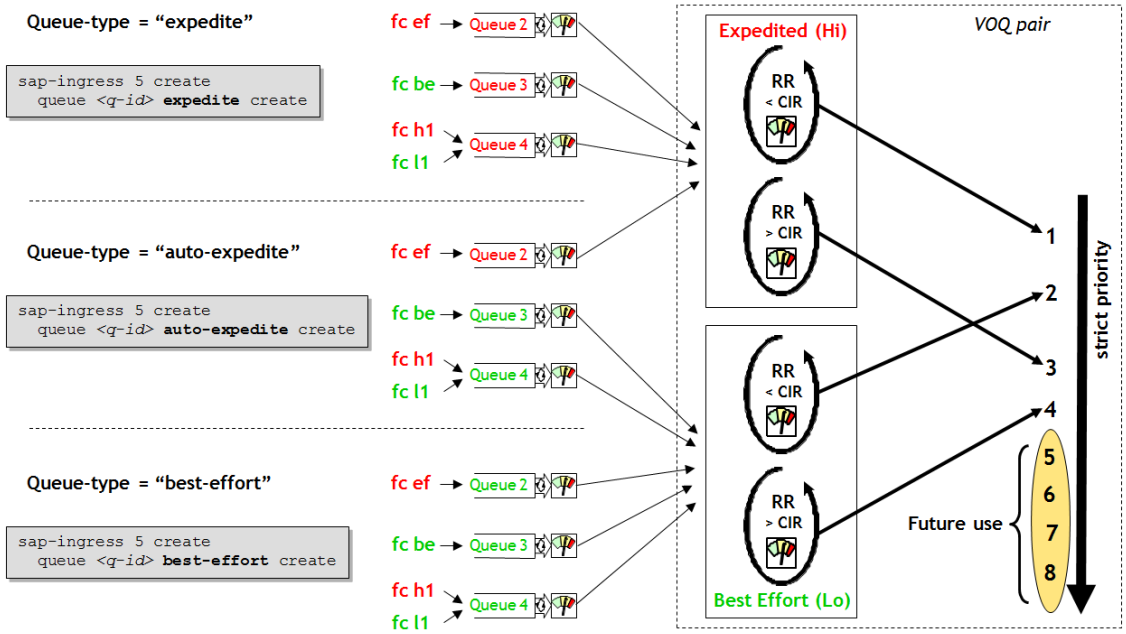


Figura 21: IOM3-XP y IMM Scheduler

En este tipo de tarjetas, se llevan a cabo 4 tipos de prioridades estrictas, siendo las dos primeras igual que en el caso anterior, la tercera de ellas la alta prioridad sobre el CIR, siendo la última la de menor prioridad por encima del valor del CIR.

Además, aparecen otras 4 prioridades latentes para otros usos.

Según los parámetros representados en la Figura 20, cada uno de ellos tendrá un comportamiento distinto a nivel de prioridad.

- Las colas de 6, 7 y 8, tiempo real, control y señalización respectivamente son colas de alta prioridad y tienen preferencia frente al resto.
- Los servicios de datos críticos, estándar y *best effort* (colas 3, 2 y 1 respectivamente), se basan en un modelo de *round robin* y serán atendidas después de las mencionadas en el punto anterior.

5.7 Gestión y mantenimiento de la red

En cuanto a las herramientas utilizadas para el mantenimiento de la red, cabe destacar las siguientes.

5.7.1 *Secure CRT 7.0*

Por su naturaleza, Telnet es un protocolo no seguro, a no ser que sean otros protocolos como IPSec los que aporten seguridad al anterior. *Secure Shell* (SHH) es un programa que proporciona la funcionalidad de Telnet pero contribuye aportando la parte de encriptación y autenticación de la que el anterior carece. Estos protocolos,

además de otros que explicaremos a continuación se complementan en una herramienta, Secure CRT.

Las funciones de la misma son, no solo la gestión sino la configuración de todos los equipos de la red, junto con sus nodos e interfaces.

5.7.2 *Simple Network Management Protocol* (SNMP)

El protocolo SNMP (*Simple Network Management Protocol*) es un requerimiento para cualquier red IP. Este protocolo opera en la capa de aplicación y su función es la de facilitar el intercambio de información de administración entre los distintos dispositivos de la red, ya san routers, *switches*, *firewalls*, etc. Permite, por tanto, supervisar el funcionamiento de la red, buscar y resolver problemas.

Al ser Alcatel-Lucent el proveedor de los equipos, SNMP estará gestionado por el servidor 5620 SAM (*Service Aware Manager*). Esta plataforma gestiona el mantenimiento de toda la red IP/MPLS y proporciona una visión a nivel de software para la infraestructura de la misma.

5.7.3 Bases de datos

El masivo uso de información que sufre la red, tiene estará gestionado por diferentes bases de datos que servirán de apoyo para ver el estado actual y pasado de la red para analizar los posibles fallos y ver la evolución que ha sufrido la misma con el fin de actuar de manera proactiva frente a futuros fallos.

Para ello, se hará uso de dos bases de datos. La primera de ellas, conocida con el nombre de *Bussiness Objects*, es una herramienta de software sobre la cual se pueden descargar archivos de los diferentes nodos e interfaces para ver su estado de ocupación y obtener un punto de vista más preciso en caso de posibles incidencias en la red. La segunda de ellas, denominada *Cacti,* es una herramienta con una funcionalidad más desde el punto de vista gráfico, en el que se podrá comprobar, entre otros, el estado y la capacidad de cada uno de los centros de la red.

6. CONCLUSIONES

This chapter will explore the conclusions and future and scalability of the project and will be supported by my opinion on the realization of the project.

6.1 Future and scalability

First of all, when it comes to the topology of the architecture, it is worth to mention that the network has been designed to achieve the following aspects:

- Reduce OPEX and CAPEX on associated WAN links by sharing common resources where ever possible.
- Ensure the reliability of SIGTRAN and voice services.
- Improve delay figures for data traffic.
- Simplify the operation of the network.
- Optimize transmission costs, keeping the network traffic balanced.

The exponential growth of the Internet and the continuous usage from the consumers, leads to the necessity of a network expansion within the following months. Therefore, the network should be able to support this impact, and thanks to the design of the physical topology, the network is flexible enough to admit additional sites or new and additional inter/intra zone capacity, if necessary. Besides the network is thought to integrate TV services in a future, where all the services will be based in IP.

In terms of the equipment, despite the fact that the network counts with perfect suitable and sustainable devices to support the amount of traffic that flows through the network, it will be a matter of time to adapt the network with the newest equipment.

Although the project is specifically designed in order to provide and facilitate communication services in the peninsula and Portugal, we do not discard the fact, and it is more than probable, that the network will expand beyond its borders, reaching not only the islands but also spreading internationally.

6.2 Conclusions

The realization of a project of this size, taking into account all the work and coordination from the different departments, had changed the way I understood a project. Despite the fact that my duty was centred in the design of the network topology with my department, I had the opportunity to submerge in the working area of the different parts, including the transmission department, Operations and

Management and network deployment, among others. Inside them, I was able to understand the environment in which they worked, even participating by providing ideas. Furthermore, since the project is related to my degree, I have managed not only to strengthen and apply my knowledge into this field, but I have also learned both technical and practical things.

To sum up, I also consider extremely beneficial working for an enterprise at this age, because it has offered me the opportunity to learn more on how the telecommunications labour market works from the inside, participating with professionals and growing both at a personal and a professional level. Besides, the implementation of this project has awakened in me the eagerness in continue working and expanding my knowledge in this field. Therefore, I would most certainly recommend the realization of a project within a company if possible.

7. PRESUPUESTO

En este apartado se expone el coste necesario para la realización del proyecto. Por un lado se incluirá el presupuesto del material empleado en el despliegue de la red y por otro, el coste personal desde el punto de vista del ingeniero. Para éste último pese a que el proyecto se ha llevado a cabo por diferentes equipos, no tiene sentido realizar un presupuesto de todas las partes. Por ello, solo se verá reflejado el impacto de una sola persona, como diseñador de proyecto.

7.1 Coste del Material

En este subapartado se incluye no solo el coste del equipamiento necesario para el despliegue de la red, sino que además se tendrá en cuenta el coste del material empleado para la realización del proyecto.

Para ello se distinguirán las siguientes partes:

- Coste del equipamiento

  Es importante resaltar que solo se incluye el coste del equipamiento hardware, obviando aquellos costes relacionados con la instalación de dichos equipos. En la siguiente tabla se resume el hardware necesario:

CONCEPTO/MODELO	PRECIO UNIDAD	NÚMERO DE EQUIPOS	TOTAL
7750 Service Router	15.000,00 €	69	1.035.000,00 €
7710 Service Router	10.000,00 €	3	30.000,00 €
7950 Extensible Routing System	45.000,00 €	6	270.000,00 €
1675 Lambda Unite MultiService Switch	7.000,00 €	12	84.000,00 €
1830 PSS	5.000,00 €	12	60.000,00 €
TOTAL			**1.479.000,00 €**

Tabla 35: Equipamiento necesario

CONCEPTO/MODELO	MODELO TARJETA	PRECIO UNIDAD	NÚMERO DE TARJETAS	TOTAL
7750 Service Router	10 GB IOM-2	3.000,00 €	4	12.000,00 €
	10 GB IOM3-XP	2.500,00 €	5	12.500,00 €
7710 Service Router	10/100 Base-T MDA	1.500,00 €	50	75.000,00 €
	10/100/1000-TX	1.500,00 €	10	15.000,00 €
	100 Base-FX	1.000,00 €	10	10.000,00 €
7950 Extensible Routing System	100GB C-XMA	5.000,00 €	20	100.000,00 €
	10GB C-XMA	2.500,00 €	100	250.000,00 €
1675 Lambda Unite MultiService Switch	10GB Ethernet Private Line	610,00 €	6	3.660,00 €
	8-port STM-1 (electrical)	290,00 €	10	2.900,00 €
1830 PSS	60GB slot	835,00 €	5	4.175,00 €
TOTAL				**485.235,00 €**

Tabla 36: Tarjetas necesaria

- Entorno de trabajo

  En esta parte se presenta el coste que supone todo el entorno de trabajo, en la oficina y todo lo que conlleva, incluyendo luz, agua y gas y material. Este coste asciende a 150€ al mes.

7.2 Coste de honorarios

En este apartado solo se contempla el coste de la persona que ha diseñado este proyecto. La duración de este proyecto se ha estimado en 5 meses a jornada completa.

Por tanto se plasma el coste de honorarios además de lo correspondiente a la propiedad industrial que supone el 0.5% del total del proyecto.

Los costes se reflejan en la siguiente tabla:

CONCEPTO	COSTE	CANTIDAD	TOTAL
Ingeniero del proyecto	150€/hora	800 horas	120.000,00 €
Propiedad industrial	0.5%	800 horas	10.421,18 €
TOTAL			**130.421,18 €**

Tabla 37: Coste honorarios

7.3 Presupuesto total

Una vez definidos todos los presupuestos por separado, se realiza un resumen del total del presupuesto, tal y como queda reflejado en la siguiente tabla.

CONCEPTO	TABLA	COSTE
Coste equipamiento routers	35	1.479.000,00 €
Coste tarjetas	36	485.235,00 €
Coste honorarios	37	130.421,18 €
TOTAL		**2.094.656,18 €**

Tabla 38: Presupuesto total

En ninguno de los costes se contempla el porcentaje del IVA correspondiente.

8. SUMMARY

Nowadays, when we think of technology, we think of smartphones, digital tablets, laptops or GPSs. It is a fact that the 21st century is facing a technological age, in which technology serves as a gateway between the world of the past and the current one, facilitating and representing our daily lives.

Thus, distance is not any more an obstacle when it comes to communication, thanks to the amount of electronic devices that makes it easier to stay in touch no matter where you are. It reduces costs and time in every aspect, and it is a source of any type of information, even for developing countries.

However, the massive usage of technology is such that the telecommunications world cannot afford to deal with this issue unless they start expanding their infrastructure.

The aim of this project is therefore to create a completely new architecture that confronts the problem mentioned above and integrate all the services in a single topology. This architecture should be capable as well of supporting the huge capacity and traffic that flows over the network. The deployment of this architecture will be carried out in Spain and Portugal, leaving apart the islands of both countries.

It is required to analyse several aspects, such as the feasibility of the project itself, the necessary equipment, the architecture design and the offered services between others. In this part, however a summary of the whole project from a high-level point of view will be included.

First of all, it is necessary to familiarise with the technology on which the architecture is based, *Multiprotocol Label Switching* or MPLS. This technology that was born in the late nineties comes from a combination of previous technologies such as IP/ATM. The continuous convergence towards IP and the performance difficulties with IP/ATM, led to the creation of new techniques named IP Switching and Multilayer Switching which were adopted by different companies. The mixture of all of them supposed the appearance of MPLS.

MPLS, thus, provides a mechanism for forwarding packets for any kind of protocol, no matter if it is ATM, Frame Relay or even Ethernet. Unlike its ancestors, MPLS is capable of harnessing in both the data and network layer, by separating the routing and forwarding functions, and as ATM, it is based on the exchange of information using labels.

This protocol works by tagging the traffic, with an identifier to distinguish the path that it should follow, known in this technology as LSP (Label Switched Path). These packets are transmitted from the origin to the destination, by the different LSRs (Label

Switched Router) that will know, depending on the labels the packets have, which LSP it should take. It then looks up the LSP in its own forwarding table to determine the best link over which to forward the packet and the label to use on this next hop. Once the packet is received by the penultimate LSR, it removes all the labels, so that the last LSR, known as Egress LSR, just has to deliver the IP packet.

Once the technology is briefly understood, it is necessary to proceed with the design of the topology and its equipment. By that, it is carried out a RFQ (Request for Quotation) to decide which hardware provider fits best to the desired services. Therefore, Alcatel-Lucent has been chosen to provide the Hardware for the project. Although it has been decided to use Alcatel-Lucent, it is important to analyse the different alternatives of equipment that this provider offers.

The need of the integration of all services together in a converged network, leads to the creation of a new model of router, known as service router. This router is a scalable internet router that offers best-effort Internet services and enables migration of traditional data and voice services on a single platform. These services such as point-to-point, multipoint virtual private LAN services (VPLS) and IP-VPNs, allow the network to attract a wider customer base at a lower cost while offering higher flexibility and quality to the user.

This is why between the different alternatives three types of routers have been selected:

- 7750 SR-12: this router has a capacity up to 1000 Gbps and represents a great advantage in the audio and video and multimedia field.

- 7950 XRS-20: this router revolutionises the Internet part, offering services such as video, cloud-computing applications and massive amount of multimedia data. At the same time it optimises costs.

- 7710 SR-c12: this router has built-in systems characteristics, flexibility and service capabilities that allow service providers to activate a new generation of high performance data services, including carrier voice and video services.

From the transmission point of view the following elements will be used:

- Alcatel-Lucent 1675 LambdaUniteMultiService Switch: it means a new generation in terms of optical switching links providing a wide range of applications, keeping at the same time a flexible, efficient in cost and manageable network.

- 1830 Photonic Service Switch: it offers multiservice transport from the Core to the rest of the network.

Although it has been decided to use equipment to implement in the deployment of the project, it should be useful to describe briefly the different elements of the proposed architecture.

First of all, the Core Layer represents, due to its name, the backbone or core of the whole architecture. This layer is responsible for providing connectivity between distribution and aggregation layer and it is composed of, what is called in MPLS, the PP (Provider P) routers. These, are paired in geographical zones in order to provide resilient connections from remote distribution and aggregation layers. It is necessary to mention that there will be two types of links in this part. The first one will be between the PPs and the other will represent the access links. In the last one, a new type of router appears called PE-C (Provider Edge). Normally, both links will be Nx10Gb/s with the exception of a certain number of sites that due to its small expected capacity will not be using the whole transmission link and therefore will be limited.

There will also be part of the network, another device called Route Reflector, responsible for the distribution of VPN-IPv4 and VPN-IPv6 BGP routes to the different PEs forming the distribution and aggregation layer at remote sites. It is worth to take into consideration that these routers will not route any customer traffic, but among other functions, it will be reflecting routes and containing Internet full-routing.

Once the architecture has been proposed, we proceed to its final deployment. The architecture of the network is called ISNET and its structure with each element is the following:

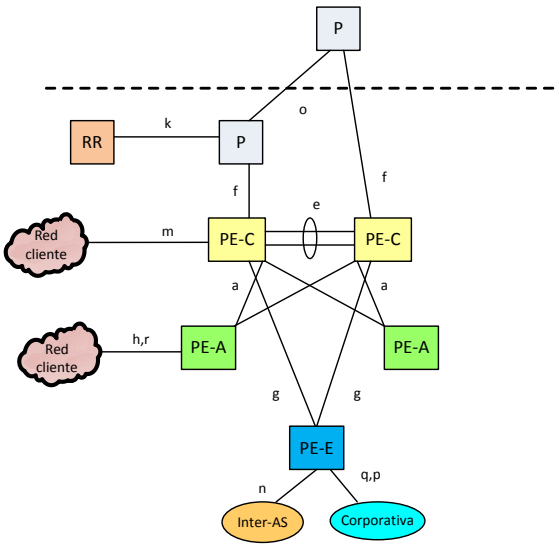


Figura 22: Physical Network Topology

According to the figure shown above we differentiate the following elements:

- P Router: routers 7750 SR-12 will be used for the implementation of the core layer, populated with 10 GE interfaces. They shall be configured with ISIS, LDP and RSVP-TE protocols.

- PE-C Router: there will be different PE-Cs whether they belong or not to the Internet part.

    - PE-C Core: routers connected directly to the Core will be 7750 SR-12, will use Fast and Gigabit Ethernet interfaces.

    - Internet PE-C: for the Internet part, two 7950 XRS-20 platform populated with a combination of 10 GE and 100 GE interfaces will be implemented. Protocols such as ISIS, LDP, RSVP-TE, MP-iBGP, OSPF, LACP and BGP shall be operating.

- PE-A Router: they will be the same model as the conventional PE-Cs, 7750 SR-12. These routers will be designated for the connection with clients. They count with a combination of 10 Gigabit Ethernet for network interfaces and Fast Ethernet/Gigabit interfaces for client access. Among its protocols, we highlight ISIS, LDP, RSVP-TE, MP-iBGP, OSPF, LACP and BGP.

- PE-E Router: the function of these routers is to provide corporative services. They will be implemented by the 7750 SR-12 platform populated with a combination of Gigabit Ethernet for network interfaces, STM-1 ports E1 and E3. They shall be configured with ISIS, LDP, RSVP-TE, IPSeC, OSPF and BGP.

- Route Reflectors: there will be 6 routers of this type, half of them for the Internet part and the other half intended to be used for the Core part, them being implemented by the 7750 SR-12 and the 7710-SRc12, respectively. They should support ISIS and MP-iBGP protocols.

Since the structure of the network has been shown from an individual point of view, it is also worth to reflect the architecture of the Core and the Internet.

As we have mentioned before, the Core part should cover redundancy and according to the need of symmetry, the P routers will be deployed in a triangular prism topology interconnected using Nx10Gb/s, as depicted in the following figure:

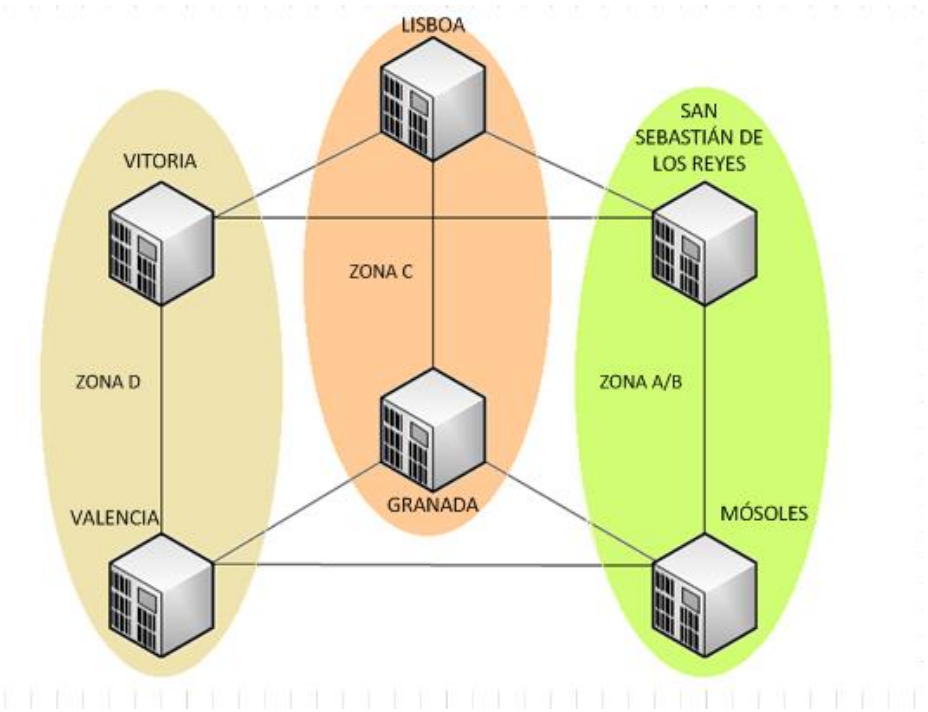


Figura 23: Core physical topology

The remote PEs forming a distribution and aggregation layer will connect to the Core P. Each site will consist of 2 inter-connected PE-C devices where each PE-C will connect to one of the control/forwarding planes providing per-site resilience to both planes. Core P router are paired and assigned to zones:

- San Sebastián de los Reyes and Móstoles from Zone A/B.
- Lisboa and Granada from Zone C.
- Vitoria and Valencia from Zone D.

Remote sites are assigned to one of these zones (based upon geographic displacement) for the purpose of determining where they connect to the core. As a general rule, each site connected to the Core layer will use Nx10Gb but as we have mentioned above, for those small sites where the traffic will not reach the 10GB transmission capacity, instead of wasting part of the link, they will be limited by using a specific number of VC4s, where each one will be disposed of 136 Mbps. In case the traffic increases in these sites, they will just need an increase in the number of VC4s.

For the Internet part, however, another topology scheme will be implemented as it is shown in the following figure:

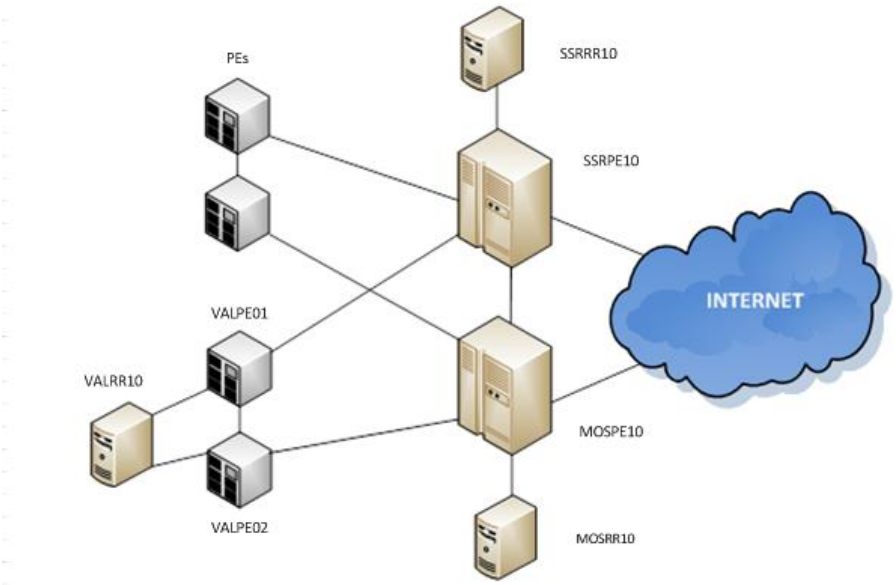


Figura 24: Internet scheme

The internet topology consists of two 7950 XRS-20 routers, located in San Sebastian and Móstoles, with their respective Route Reflector connected to each one. Half of the PEs from the distribution and aggregation layer will be connected to both internet routers. It is important to mention that a third Route reflector, connected to Valencia, will be part of the internet architecture.

9. REFERENCIAS BIBLIOGRÁFICAS

Entre las referencias bibliográficas utilizadas durante la ejecución de este proyecto cabe destacar:

{1} RFC 1918 Address Allocation for Private Internets

https://tools.ietf.org/html/rfc1918

{2} RFC 3031 Multiprotocol Label Switching Architecture

https://tools.ietf.org/html/rfc3031

{3} RSVP-TE: Extensions to RSVP for LSP Tunnels

https://tools.ietf.org/html/rfc3209

{4} Fast Reroute Extensions to RSVP-TE for LSP Tunnels

https://tools.ietf.org/html/rfc4090

{5} Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)

https://www.ietf.org/rfc/rfc4365

{6} Alcatel-Lucent

https://www.alcatel-lucent.com/

{7} Agencia Estatal Boletín Oficial del Estado

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950

{8} CNMC

http://www.cnmc.es/

{9} La nueva Ley General de Telecomunicaciones

http://www.ticbeat.com/economia/la-nueva-ley-general-de-telecomunicaciones/

{10} Slope QoS Policies 7750-SR

https://infoproducts.alcatel-lucent.com/html/0_add-h-f/93-0077-10-01/7750_SR_OS_QoS_Guide/QoS-slope-policy.pdf

{11} Alcatel-Lucent 7750 SERVICE ROUTER DATA SHEET

https://lafibre.info/images/datacenter/201209_alcatel-lucent_7750_sr_ms-isa.pdf

{12} Alcatel-Lucent 7710 SR DATA SHEET

http://lightspeedt.com/wp-content/uploads/2011/06/7710SR%20-%20DataSheet.pdf

{13} ALCATEL-LUCENT 7950 EXTENSIBLE ROUTING SYSTEM

http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2013/6432-7950-xrs-family-datasheet.pdf

{14} Alcatel-Lucent 1675 LambdaUnite MSS

http://lightspeedt.com/wp-content/uploads/2011/06/1675_LambdaUnite-DataSheet.pdf

{15} ALCATEL-LUCENT 1830 PHOTONIC SERVICE SWITCH

http://www.netnordic.se/wp-content/uploads/2014/09/1830-PSS-16-32-R7-Datasheet.pdf

{16} Over The Top

http://mundocontact.com/plataformas-de-servicios-ott-la-cuarta-ola-tecnologica/

10. GLOSARIO

- **AppleTalk:** un conjunto de protocolos desarrollados por Apple Inc. para la interconexión de redes locales.
- **ATM:** *Asynchronous Transfer Mode,* es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.
- **Backhaul:** una red de retorno, que representa la parte de una red jerárquica entre los enlaces intermedios entre el Core (*backbone)* y el resto de subredes.
- ***Best-Effort***: Servicio que reciben los flujos que no han podido establecer una reserva de recursos en el que todos los usuarios reciben el mejor servicio posible. Este tipo de servicio se corresponde con el default PHB en DiffServ.
- **BGP**: Border Gateway Protocol es un protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas autónomos.
- **CBS**: *Committed Burst Size*, garantiza el tamaño de la ráfaga en una cola.
- **CIR:** *Committed information rate*, define el porcentaje sobre el que el sistema prioriza una cola frente al resto por el ancho de banda.
- **CSPF:** *Constrained Shortest Path First*, es una extensión del SPF con ciertas restricciones. Emplea *routing* de tipo CBR.
- **DWDM:** *Dense Wavelength Division Multiplexing* es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550nm). Se basa en la multiplexación de diferentes longitudes de onda.
- **E1:** correspondiente europeo del T1, se trata de una tasa de transmisión de 2048 Mbit/s capaz de soportar 32 canales PCM, 30 de ellos para voz y los dos restantes para señalización.
- **E3:** un tipo de multiplexación SDH con una tasa de transmisión de 34 Mbit/s.
- **EIR**: *Excess information rate*, es una tasa extra de ancho de banda que se da en determinadas situaciones.
- **Ethernet:** es el diseño de una red de área local, que se basa en la transmisión en banda base y que emplea el protocolo CSMA/CD como método para el control de acceso.
- **Flujo:** Secuencia de datagramas relacionados resultantes de una actividad de usuario única que requieren la misma QoS.
- **Frame Relay**: técnica de comunicación basada en la conmutación de paquetes que transmite una variedad de tamaños de tramas para datos, perfecto para grandes cantidades de datos.
- **FTTH:** *Fiber to the Home.*

- **IGP:** *Interior Gateway Protocol* o protocolo de pasarela interno, hace referencia a los protocolos usados dentro de un sistema autónomo.
- **IGRP**: *Interior Gateway Routing Protocol*¸ es un protocolo que se utiliza como IGP para el intercambio de datos dentro de un Sistema autónomo.
- **IP:** *Internet Protocol* es un protocolo de comunicación de datos digitales de la capa de red, según el modelo internacional OSI. Su función es la transmisión de información mediante un protocolo no orientado a conexión.
- **IPsec:** *Internet Protocol security*, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete IP en el establecimiento de claves de cifrado.
- **IPX:** *Internetwork Packet Exchange,* es un antiguo protocolo de comunicaciones de redes NetWare utilizado para transferir datos de un nodo a otro de la rede mediante paquetes de datos llamados datagramas.
- **ISP:** *Internet Service Provider* o proveedor de servicios de internet, es la empresa que ofrece conexión a Internet a sus clientes, es decir, conecta a sus usuarios a Internet a través de diferentes tecnologías como ADSL, cablemódem, GSM, dial-up, etcétera.
- **Jitter:** Variabilidad del retardo de los paquetes dentro de un mismo flujo.
- **Jumbo frames:** son tramas Ethernet con más de 1500 bytes de carga, hasta un total de 9000 bytes.
- **LACP:** *Link Aggregation Control Protocol*.
- **Lookback:** se trata de una interfaz de red virtual normalmente utilizada para probar la capacidad de la tarjeta interna si se están enviando datos BGP. Esta dirección también se suele utilizar cuando una transmisión de datos tiene destino el propio host.
- **LSR:** *Label Switch Router*, son aquellos routers MPLS responsables del *switching* de etiquetas para el reenvío de paquetes.
- **MBS**: *Máximun Burst Size*, define el buffer máximo establecido en una cola.
- **Métrica:** valor que asigna un dispositivo de red como un router para evaluar el coste de una ruta.
- **MTU**: *Máximum Transfer Unit,* es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.
- **Multicast**: se refiere al envío de la información en múltiples redes a múltiples destinos simultáneamente.
- **OSI:** *Open System Interconnection,* es un modelo de referencia para los protocolos de red de arquitectura en capas.
- **OSPF**: *Open Shortest Path First,* es un protocol de encaminamiento jerárquico, como IGP, que usa el algoritmo de Dijkstra para calcular la ruta óptima.

- **PDU:** *Protocol Data Unit* o protocolo de unidad de datos, se utilizan para el intercambio de datos entre unidades disparejas.
- **PIM:** *Protocol independent multicast*, es un protocolo de encaminamiento que crea una estructura de árbol de distribución entre los clientes *multicast* formando dominios.
- **PIR**: *Peak information rate*, es la tasa de ancho de banda o rendimiento, cuyo valor es la suma del CIR y el EIR.
- **PPP**: *Point-to-Point Protocol,* es un protocolo de nivel de enlace de datos, usado para el establecimiento de una conexión directa entre dos nodos de una red de computadores.
- **QoS:** *Quality of Service.*
- **RDI:** *Remote Defect Indication,* es un método de señalización de un error.
- **RFQ**: *Request for Quotation* o solicitud de cotización, es un documento que contiene la información y especificaciones en el momento en el que una empresa solicita a las empresas proveedoras para crear un presupuesto exacto y competitivo.
- **RIP:** *Routing Information Protocol,* es un protocolo IGP utilizado por los routers para el intercambio de información acerca de redes IP a las que se encuentran conectados.
- **SCTP:** *Streaming Control Transport Protocol*, es un protocolo de comunicación de la capa de transporte creado para Sigtran.
- **SDH:** *Synchronous Digital Hierarchy*, es un conunto de protocolos de transmisión de datos mediante la fibra óptica.
- ***SIGTRAN****: SIGTRAN* se refiere a una pila de protocolos para el transporte de protocolos de señalización (SS7/C7) de la red de conmutación de circuitos (SCN) (cuya aplicación más clásica es telefonía pública) sobre una red IP. SIGTRAN es la evolución de SS7, que define los adaptadores y una capacidad de transporte básico donde se mezclan protocolos SS7 y de paquetes para ofrecer a los usuarios lo mejor de ambas tecnologías. Aplicaciones de SIGTRAN incluyen: Internet por Dial-Up, telefonía IP interconectada con *PSTN* y otros servicios.
- **SLA**: *Service Level Agreement* o acuerdo de nivel de servicio, es un contrato entre un ISP y su cliente con el objetivo de fijar el nivel acordado para la calidad de dicho servicio.
- **SNA:** *Systems Network Architecture,* es una arquitectura de red diseñada por IBM diseñada para la conectividad con hosts o con grandes servidores de IBM.
- **SONET:** *Synchronous Optical Network,* es un estándar para el transporte de telecomunicaciones en redes de fibra óptica.
- **STM-1:** unidad de transmisión basada en SDH correspondiente al primer nivel básico ofreciendo una capacidad de 155 Mbit/s.

- **TCP:** *Transmission Control Protocol,* es uno de los protocolos fundamentales en Internet, usado para establecer conexiones entre redes de computadores para enviarse un fujo de datos. Se caracteriza por garantizar que los datos serán recibidos sin errores y ordenados.
- **VC4:** tipo de contenedor virtual de nivel 4 propio de las rutas SDH.
- **VPLS:** *Virtual Private Lan Service*, es una red privada virtual, es decir una VPN, que permite conectividad multipunto.